



**Certification for FCC Approval
for Use With the Broadcast Flag**

Submitted by: THOMSON, on behalf of itself and the following companies supporting the **SmartRight** system:
AXALTO
GEMPLUS SA
MICRONAS
NAGRAVISION SA
PIONEER CORPORATION
SCM MICROSYSTEMS
ST MICROELECTRONICS N.V.

March 1, 2004

Federal Communications Commission
Office of the Secretary
Att: Broadcast Flag Certifications
c/o Natek, Inc.
236 Massachusetts Avenue, N.E.
Suite 110
Washington, D.C. 20002

Re:



Dear Ms. Dortch:

Thomson, on behalf of itself and Axalto, Gemplus S.A., Micronas, Nagravision S.A., Pioneer Corporation, SCM Microsystems, and ST Microelectronics N.V., companies that support the SmartRight system, is pleased to submit for the Commission's consideration a Broadcast Flag technology certification for "**SmartRight**." **SmartRight** is an encryption-based digital broadcast content protection system that recognizes and gives effect to the "Broadcast Flag" for the purpose of preventing unauthorized, indiscriminate redistribution of digital broadcast content over the Internet, in conformance with FCC rules.

The attached Broadcast Flag Certification includes information and documentation to permit the Commission to evaluate **SmartRight** consistent with the elements requested in its January 23, 2004 Public Notice (DA 04-145) ("Broadcast Flag Certification Public Notice"). This includes: a general description of how **SmartRight** works, including its scope of redistribution; a detailed analysis of the level of protection **SmartRight** affords to digital broadcast content; information regarding the extent to which content owners, broadcasters, or equipment manufacturers have expressed support for **SmartRight**; and a copy of **SmartRight's** licensing terms and fees, which evidence that the technology will be licensed on a reasonable and non-discriminatory basis.



March 1, 2004

Page 2

In accordance with the Broadcast Flag Certification Public Notice, an original and four copies of the **SmartRight** Broadcast Flag Certification are being filed by hand with the Commission, and a copy also has been delivered to Mr. W. Kenneth Ferree, Chief, Media Bureau. I would be pleased to respond to any questions you may have regarding this matter.

Respectfully Submitted,

David H. Arland
Vice President
U.S. Corporate Communications & Government Relations

Enclosure: SmartRight Broadcast Flag Certification (one original and four copies)

cc (with enclosure): W. Kenneth Ferree
William H. Johnson
Rick Chessen
Susan Mort
John Wong

DISCLOSURE

This document is provided “as is” with no warranties whatsoever, including any warranty of merchantability, non-infringement, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification or sample.

Thomson, Axalto, Gemplus SA, Micronas, Nagravision SA, Pioneer Corporation, SCM Microsystems, and ST Microelectronics N.V. disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information of this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Copyright © 2004 by Thomson, Axalto, Gemplus SA, Micronas, Nagravision SA, Pioneer Corporation, SCM Microsystems, and ST Microelectronics

SmartRight is a trademark of Thomson. Third party brands and names are the property of their respective owners.

TABLE OF CONTENTS

| | | |
|-------|---|----|
| 1 | Executive Summary | 1 |
| 2 | Purpose and Effect of the Broadcast Flag | 5 |
| 2.1 | Prevent Indiscriminate, Unauthorized Redistribution of DTV Over The Internet..... | 5 |
| 2.2 | Maximize Consumers' Use and Enjoyment of DTV Within That Basic Constraint | 5 |
| 3 | SmartRight Accomplishes The Broadcast Flag Objectives | 6 |
| 3.1 | SmartRight's Innovative "Authorized Domain" Approach Offers End-to-End Protection from Reception to Display and Thwarts Indiscriminate Unauthorized Internet Redistribution..... | 6 |
| 3.2 | SmartRight's "Private Personal Network" Architecture Preserves The "Copy Freely" Environment For DTV Content, And Enhances Consumers' Use and Enjoyment of DTV By Permitting Secure, Discriminating Internet Redistribution of Protected DTV Content To A Second Home, Car, Boat or Office..... | 7 |
| 4 | System Overview | 8 |
| 4.1 | End-To-End Protection Within the Personal Private Network | 8 |
| 4.2 | Prevention of Unauthorized, Indiscriminate Redistribution Over The Internet..... | 8 |
| 4.3 | Reception, Display & Storage Devices | 9 |
| 4.4 | Secure Modules | 10 |
| 4.5 | Usage States | 10 |
| 4.6 | Renewability..... | 10 |
| 4.7 | Revocation..... | 11 |
| 4.8 | Interoperability | 11 |
| 5 | Level of Security Provided..... | 12 |
| 5.1 | SmartRight Personal Private Network | 12 |
| 5.2 | End-to-End Protection..... | 12 |
| 5.3 | Preventing Indiscriminate Redistribution Over The Internet..... | 13 |
| 5.4 | Proximity Control..... | 13 |
| 5.5 | Local Enforcement Copy-Management Message | 14 |
| 5.6 | Enforcement of Usage Rights..... | 14 |
| 5.6.1 | Copy Freely | 14 |
| 5.6.2 | Private Copy | 15 |
| 5.7 | Security analysis..... | 15 |

| | | |
|-------|---|----|
| 5.7.1 | Trust Model | 15 |
| 5.7.2 | Security Mechanisms | 15 |
| 5.7.3 | Protocols..... | 16 |
| 5.7.4 | Proposed Algorithms..... | 16 |
| 5.8 | Copyright Watermark..... | 16 |
| 6 | Renewability and Revocation..... | 18 |
| 6.1 | Protection Against Circumvention Devices | 18 |
| 6.2 | Renewability And Resistance To Obsolescence | 18 |
| 6.3 | Revocation..... | 18 |
| 7 | Interoperability | 20 |
| 8 | Consumer Use and Enjoyment..... | 21 |
| 8.1 | SmartRight Preserves The “Freely-Copiable” Environment..... | 21 |
| 8.2 | SmartRight Enhances Consumers’ Use and Enjoyment of DTV By Permitting Secure, Discriminating Internet Redistribution of Protected DTV Content To A Second Home, Car, Boat or Office | 21 |
| 8.3 | SmartRight Preserves the Functionality of Legacy Devices | 21 |
| 9 | The SmartRight License..... | 22 |
| 9.1 | Overview | 22 |
| 9.2 | Structure of Agreement | 23 |
| 9.3 | Fees..... | 23 |
| 9.4 | Reciprocal Licensing..... | 23 |
| 9.5 | Approval Process..... | 23 |
| 9.6 | Confidentiality..... | 24 |
| 9.7 | Changes | 24 |
| 9.8 | Term and Termination..... | 24 |
| 9.9 | Disclaimer And Limitation of Liability..... | 24 |
| 9.10 | Remedies | 24 |
| 9.11 | Revocation and Renewal..... | 24 |
| 9.12 | Compliance Rules Applicable to Unencrypted Digital Broadcast Content | 25 |
| 9.13 | Robustness Rules..... | 25 |
| 10 | Marketplace Support for SmartRight | 26 |

TABLE OF FIGURES

| | |
|---|----|
| Figure 1: SmartRight ’s Broadcast Flag environment..... | 9 |
| Figure 2: Marked content within the SmartRight authorized domain | 13 |



TABLE OF TABLES

| | |
|---|----|
| Table 1: List of used abbreviations | 27 |
|---|----|

| | |
|-------------|--|
| APPENDIX A: | The SmartRight License Agreement (March 1, 2004) |
|-------------|--|

1 Executive Summary

The **SmartRight** digital content protection system (“**SmartRight**”) accomplishes the FCC’s objectives in adopting its Broadcast Flag regime by offering content owners a secure and pervasive method, employing multiple redundancies, by which to protect their digitally-broadcast works from indiscriminate redistribution over the Internet, and by not only preserving, but even *enhancing*, consumers’ use and enjoyment of DTV.

SmartRight Protects The Interests of Content Owners

SmartRight prevents digital broadcast content from indiscriminate, unauthorized redistribution, including over the Internet, outside a secure, authorized domain of devices known as a Personal Private Network (“PPN”). Once received into the Personal Private Network by a **SmartRight**-enabled receiver, **SmartRight**-protected content cannot be redistributed over the Internet without **SmartRight** redistribution control, which effectively renders that content useless (that is, unviewable) by any recipient outside the Personal Private Network, including even those with a different **SmartRight** Personal Private Network. Moreover, unlike the traditional “chain of protection” approach taken by other encryption-based digital content protection technologies, wherein marked content is successively encrypted and decrypted within the personal digital network, **SmartRight** provides “end-to-end” protection from the moment the content is received and throughout its movement within the Personal Private Network. **SmartRight** also offers multiple redundant security features, including “proximity controls” and an available copyright watermark for analog content, further safeguarding digital broadcast content from indiscriminate redistribution over the Internet.

SmartRight Protects The Interests of Consumers

Within his or her own Personal Private Network, a consumer may enjoy viewing protected digital content from any of his or her display devices, as well as freely copying protected digital broadcast content on both non-removable and removable storage media. In this manner, **SmartRight** preserves consumer expectations that the DTV transition will not be a step *backward* in terms of their use and enjoyment of broadcast television programming. However, recognizing that consumers rightly expect to enjoy *more* flexibility with DTV than they have with today’s analog television, **SmartRight** goes a step further by enabling the consumer to send protected DTV content over the Internet, securely and discriminately, to remote devices within his or her Personal Private Network, such as in a second home, office, car or boat. **SmartRight**’s consumer-friendly “Smart Card” renewability system, and its full interoperability with legacy analog television equipment further underscores its keen focus on satisfying the needs and expectations of American consumers.

SmartRight Is Universally Interoperable

The **SmartRight** system is capable of operating either independently as a self-contained system, or beside or on top of other digital content protection systems. **SmartRight** is interoperable with other FCC-approved Broadcast Flag digital content protection systems, digital content delivery systems designed for cable and satellite conditional access systems, telco/broadband delivery systems, and any other digital signaling network with access to the home. It protects pre-recorded media (*e.g.*, DVDs), is not dependent on any specific interface (IP, WiFi, Firewire,

USB, etc.) and supports multimedia formats such as MPEG-2, MPEG-4 or mp3Pro, etc. As mentioned, **SmartRight** in no way diminishes the functionality of legacy television equipment.

Key SmartRight Attributes

- **Prevention of Indiscriminate Redistribution Over The Internet:** Once content has been encrypted by **SmartRight**, it cannot be redistributed over the Internet (or to a different Personal Private Network) without retaining its **SmartRight** redistribution control (*i.e.*, encryption). Outside the Personal Private Network, including in the case of attempted indiscriminate redistribution over the Internet, digital content encrypted by **SmartRight** remains encrypted, and therefore unviewable on any device outside the PPN, including those within a different **SmartRight** PPN.
- **End-To-End Protection Within The Personal Private Network:** Unlike “piecemeal” approaches, which combine link encryption schemes (protecting content transferred between devices) and storage encryption schemes (protecting content within devices), the **SmartRight** system adopts a global approach, employing a seamless, end-to-end encryption scheme over an entire digital home network – the Personal Private Network – which is an authorized digital network of **SmartRight** devices linked through wired or wireless digital connections. Under this innovative approach, “flagged” digital broadcast content is encrypted upon its reception and throughout the PPN; decryption occurs only when the content is displayed.
- **Redundant, State-of-The-Art Security Mechanisms:** **SmartRight** incorporates multiple, mutually-reinforcing security mechanisms and techniques to protect DTV content. These include: the most attack-resistant cryptographic protocols and algorithms; “Proximity Control,” which restricts – on a geographic basis – even discriminating transmissions of **SmartRight**-encrypted content over the Internet, thus protecting content owners’ rights vis-à-vis secondary and foreign markets; and an optional dedicated “Copyright Watermark,” which broadcasters or content providers can add to **SmartRight**-protected content to protect against indiscriminate redistribution over the Internet of protected digital content that has been exported to an analog output.
- **Defenses Against Circumvention:** **SmartRight** protects against “cloned” Smart Cards, fake terminal cards using a regular certificate, rogue host devices with tampered copy protection means (e.g., with digital output copy protection disabled); large-scale impersonation of a host device by a PC; and “crackers” having retrieved one network key and making use of it (e.g., distribution of content in-the-clear).
- **“Smart Card” Renewability:** **SmartRight** offers the effectiveness and simplicity of “Smart Card” system renewal, which is not only extremely effective and pervasive in protecting content from indiscriminate redistribution over the Internet, but also remarkably consumer-friendly, in the event of a device-specific – or even a system-wide – compromise. In the event of a system-wide attack, **SmartRight** offers true renewability, requiring only the replacement of secure, removable modules, or “Smart Cards.” Consumers never have to change their **SmartRight** devices after a lethal hack.
- **Multi-Level Revocation:** In cases where only an individual device is compromised (thus not requiring renewability of the entire system), **SmartRight** implements a three-level revocation mechanism, including: (1) PPN Revocation (wherein every device within a revoked PPN will not be able to handle **SmartRight** content); (2) Smart Card

Revocation (in which other security modules will not collaborate with the revoked device); and (3) Display Device Revocation (in which content will not be passed to a revoked display device).


- **Consumer Use and Enjoyment Within the PPN:** **SmartRight** permits consumers to copy freely digital broadcast content for lawful, personal use, just as they have become accustomed to doing with analog broadcast content. Within the PPN, the consumer is free to view, record and in all other ways enjoy DTV content without limitation. In addition to permitting access to and enjoyment of protected digital broadcast content within the home, **SmartRight** enables the consumer to include devices in remote locations, such as a car, second home, office or boat, within his/her PPN, and to transmit **SmartRight**-protected content to those devices over the Internet via a secure, discriminating transmission.

The SmartRight License Also Protects Consumers, Competition and Content Owners

SmartRight will be licensed on a reasonable and non-discriminatory basis.¹ The **SmartRight** license safeguards the legitimate interests of consumers in their use and enjoyment of digital broadcast content within his or her Personal Private Network, protects the legitimate interests of equipment manufacturers in a competitive marketplace for both digital television products and digital content protection technologies, and provides content providers with a robust system that will provide outstanding protection against unauthorized redistribution of their works and the legal means to enforce their rights on third party beneficiaries. Some examples of such provisions include:

- Implementation of a Personal Private Network that permits consumers to display content received by them on a variety of devices both within their homes and elsewhere, while still preventing unauthorized indiscriminate dissemination over the Internet and outside of the user's Personal Private Network.
- Provision for full compatibility with other approved digital content protection systems, so that consumers will not lose the use of legacy devices or the ability to view content on non-**SmartRight** devices that provide alternative means of approved protection.
- The ability to revoke individual keys coupled with procedural protections to protect consumers against unfair or erroneous use of that capability;
- A renewal process which permits a general replacement of any compromised technology without adversely affecting the interests of consumers;
- Limitations on changes to the specification and compliance rules that would adversely impact equipment manufacturers and procedural protections for adopters to safeguard competition, patterned after the DFAST license used in connection with unidirectional digital cable-ready products;

¹ The **SmartRight** License Agreement (included as Appendix A), in addition to Broadcast Flag provisions, also contains copy control provisions relevant to the protection of non-broadcast content delivered over cable and direct broadcast satellite systems.

-
- 
- The granting of an option to adopters who have essential patents to preserve their intellectual property rights subject only to an obligation to license their fellow adopters on reasonable and non-discriminatory terms, again, consistent with the approach taken in the DFAST license;
 - A qualification procedure which permits manufacturers to self-certify their products as compliant while preserving overall supervision and quality control;
 - The granting of express third party rights to digital broadcast content providers to enforce the agreement;
 - Full potential for the implementation of an analog watermark protection system.
 - Compliance rules that are specifically tailored to the particular requirements of publicly disseminated broadcast content, while still affording a broad range of protection to commercial audio-visual content originating from a wide variety of other services and media.
 - Robustness rules that conform to the FCC's "ordinary user" standard.

2 Purpose and Effect of the Broadcast Flag

2.1 Prevent Indiscriminate, Unauthorized Redistribution of DTV Over The Internet

In adopting a digital broadcast content protection regime, the FCC seeks to prevent the indiscriminate redistribution of digital television broadcast content (“DTV”) over the Internet. In doing so, the FCC recognized that, absent such a content protection regime, content owners will be unlikely to make readily available their digital content over broadcasting outlets – an outcome that could significantly damage the success of the DTV transition and the future viability of over-the-air broadcasting.

2.2 Maximize Consumers’ Use and Enjoyment of DTV Within That Basic Constraint

One of the paramount objectives in the transition to digital television has been to ensure that consumers’ experience with digital television is not only a positive one, but far superior than what they have today with analog television. In addition to benefiting from radical improvements in picture quality and sound, consumers expect the digital TV experience to be one that offers greater – or, at a minimum, no less – flexibility with regard to their use and enjoyment of digital broadcast content, including through the use of new devices, such as digital video recorders and DVD recorders. This includes – as the FCC expressly envisions in its *Report and Order* – enabling consumers to use the Internet to send digital broadcast content (e.g., to a remote personal environment, such as a second home or office) *where that content can be adequately protected from indiscriminate redistribution*.

3 SmartRight Accomplishes The Broadcast Flag Objectives

The **SmartRight** digital content protection system (“**SmartRight**”) accomplishes the objectives of the FCC’s Broadcast Flag regime, preventing digital broadcast content from indiscriminate, unauthorized redistribution, including over the Internet, outside a secure, authorized domain of devices, known as a “Personal Private Network;” and preserves – indeed, *enhances* – consumers’ use and enjoyment of DTV by expanding the scope of devices included in this network to those in a consumer’s car, second home, boat or office.

3.1 SmartRight’s Innovative “Authorized Domain” Approach Offers End-to-End Protection from Reception to Display and Thwarts Indiscriminate Unauthorized Internet Redistribution.

The **SmartRight** content protection system is designed to secure entertainment media (in this case, digital broadcast content)² within a network of authorized devices known as the Personal Private Network (“PPN”). A Personal Private Network is a limited set of devices, belonging to a family or an authorized network domain, which are linked through wired or wireless digital connections. Within his/her own Personal Private Network, a consumer may enjoy viewing content from any of his/her display devices. Nevertheless, once received, **SmartRight**-protected content cannot be redistributed over the Internet without **SmartRight** redistribution control, which renders that content useless (that is unviewable) by any recipient outside the PPN, including those with a different **SmartRight** Personal Private Network. Moreover, unlike the traditional “chain of protection” approach taken by other encryption-based digital content protection technologies, wherein marked content is successively encrypted and decrypted within the personal digital network, **SmartRight** provides a secure and seamless blanket of protection from the moment the content is received, throughout its movement within the Personal Private Network.

² In addition to protecting over-the-air digital content using the Broadcast Flag, **SmartRight** is capable of securing (both in terms of preventing indiscriminate redistribution over the Internet and appropriately limiting content-specific copying) media delivered to the home via cable, direct broadcast satellite, telco operator retransmission, or by any digital signalling network with access to the home (see discussion in Section 7).

3.2 SmartRight's "Private Personal Network" Architecture Preserves The "Copy Freely" Environment For DTV Content, And Enhances Consumers' Use and Enjoyment of DTV By Permitting Secure, *Discriminating* Internet Redistribution of Protected DTV Content To A Second Home, Car, Boat or Office

SmartRight entirely preserves, for digital broadcast content, the "copy freely" environment consumers enjoy today with analog broadcast content. Within a **SmartRight** Personal Private Network, consumers will be able to copy – both with respect to non-removable storage media (*i.e.*, hard drives) and removable storage media (*i.e.*, recordable DVDs) – protected DTV content and then view that content on any display device within the Personal Private Network.

In addition, **SmartRight** greatly enhances consumer use and enjoyment of DTV by enabling consumers to enjoy **SmartRight**-protected DTV content on remote devices – such as in a second home, car, office or boat – either by way of **SmartRight**-protected removable media or via secure and discriminating redistribution over the Internet.

In addition, by offering many levels of interoperability (including with other FCC-approved Broadcast Flag content protection systems, other content delivery systems (*e.g.*, cable and satellite conditional access systems), many content formats, and any two-way digital bus) and the simplicity of "smart card" system renewal, **SmartRight** represents digital broadcast content protection that is not only extremely effective and pervasive in protecting content from indiscriminate redistribution over the Internet, but also remarkably consumer-friendly, especially in the event of a device-specific – or even system-wide – compromise.

4 System Overview

SmartRight is an encryption-based digital broadcast content protection system that recognizes and gives effect to the “Broadcast Flag” (a.k.a. Redistribution Control descriptor (rc_descriptor())) described in ATSC Standard A/65B: “Program and System Information Protocol for Terrestrial Broadcast and Cable”) for the purpose of preventing unauthorized, indiscriminate redistribution of digital broadcast content over the Internet.

4.1 End-To-End Protection Within the Personal Private Network

Unlike “piecemeal” approaches, which combine *link encryption schemes* (protecting content transferred between devices) and *storage encryption schemes* (protecting content within devices), the **SmartRight** system is a global approach, employing a seamless, end-to-end encryption scheme over an entire digital home network, the Personal Private Network, which is an authorized digital network of **SmartRight** devices linked through wired or wireless digital connections.

Under this innovative approach, “flagged” digital broadcast content is encrypted upon its reception and throughout the Personal Private Network; decryption occurs only when the content is displayed. The consumer, meanwhile, is free to view, record and in all other ways enjoy DTV content without limitation within his or her PPN. Notably, in addition to permitting access and enjoyment of protected digital broadcast content within the traditional confines of a local domain of authorized devices (*i.e.*, those within a single home), **SmartRight** allows the consumer to include remote locations, such as a car, second home, office or boat within his/her PPN, and to transmit **SmartRight**-protected content to those devices over the Internet via a secure, discriminating transmission.

4.2 Prevention of Unauthorized, Indiscriminate Redistribution Over The Internet

Once content has been encrypted by **SmartRight**, it cannot be redistributed either to a different Personal Private Network, or over the Internet without retaining its **SmartRight** redistribution control (*i.e.*, encryption). Outside the Personal Private Network, including in the case of attempted indiscriminate redistribution over the Internet, digital content encrypted by **SmartRight** remains encrypted, and therefore unviewable on any device outside the PPN, including those within a different **SmartRight** PPN.

In addition, the availability of an optional © Copyright watermark, if added by the broadcaster, will render unviewable any protected content that has been exported through an analog output, including when that content has been redistributed over the Internet.

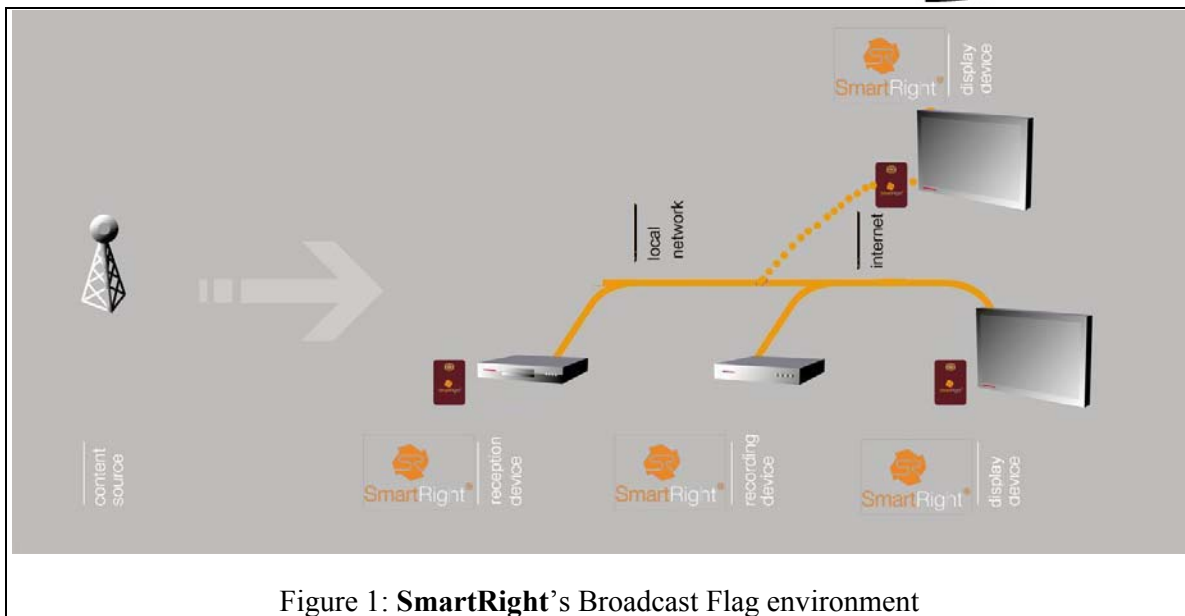


Figure 1: **SmartRight**'s Broadcast Flag environment

Figure 1 shows the Broadcast Flag environment of the **SmartRight** system. There are two domains of protection: the delivery domain and the **SmartRight** domain.

4.3 Reception, Display & Storage Devices

SmartRight-enabled devices carry out at least one of three roles:

- **Reception** – A **SmartRight** reception device is equipped to demodulate ATSC DTV signals and, as such, is a gateway for over-the-air digital broadcast content. All **SmartRight** reception devices are equipped to recognize and give effect to the Broadcast Flag. **SmartRight** will always screen digital broadcast content prior to any digital output to determine if it is marked or unmarked. Once a **SmartRight** compliant receiver detects the presence of the Broadcast Flag, it encrypts the content as Private Copy for distribution within the digital home network.
- **Display** – A **SmartRight** display device renders **SmartRight**-protected digital broadcast content for display or exports that content to an FCC-approved digital content protection system. A display device will not process marked content received over the Internet without **SmartRight** redistribution control. When exporting content, **SmartRight** conveys the content's Broadcast Flag status to the content protection technology in charge of the exportation.
- **Storage** – A **SmartRight** storage device records and stores content carried over the network. Since content protected by the **SmartRight** system is only decrypted when it is displayed, it always remains protected while stored.

SmartRight-enabled devices may combine two or more functionalities, such as reception and display (e.g., an Integrated Digital TV), storage and display (e.g., a Personal Video Recorder integrated with a display device), or reception and storage (e.g., a DVD player or DVD recorder).

4.4 Secure Modules

To achieve both efficient protection and renewable security, the **SmartRight** system uses *embedded or removable secure modules*. **SmartRight** modules may be an embedded tamper resistant module or a tamper resistant, removable National Renewable Security Standard (NRSS) card, or ISO-7816 “smart card.” Such modules securely store the secret keys and safely perform associated cryptographic processing.

Within the **SmartRight** architecture, the secure module is a Converter Module (in the reception device) and a Terminal Module (in the display device):

- At the reception end, the *Converter Module* embeds the usage state (as discussed below, in the Broadcast Flag context, these states include “copy freely” and “private copy”) and scrambling keys into a protected data structure called a Local Enforcement Copy-Management Message (LECM). A reception device can send this information together with content within the Personal Private Network.
- At the other end of the network, the *Terminal Module* decrypts the information within a display device. Based on the usage state, a Terminal Module can enable descrambling of the protected content by the display. Again, in the Broadcast Flag context, DTV content will be freely viewable within the Personal Private Network.

4.5 Usage States

With respect to digital broadcast content, the **SmartRight** system supports two usage states: “Copy-freely” and “Private-Copy.”

- Copy Freely – digital content without the presence of the Broadcast Flag will be marked “copy freely” and may be freely copied by the consumer and redistributed to other **SmartRight** PPNs for viewing or storing.
- Private Copy – digital broadcast content containing the Broadcast Flag will be marked “private copy” and may be freely copied by the consumer within his or her PPN but cannot be redistributed, either to other **SmartRight** PPNs or indiscriminately over the Internet, in a viewable manner. “Private-copy” content can only be viewed within the PPN where it has been created.

4.6 Renewability

In case of a class attack, in which each device is compromised, **SmartRight** proposes true renewability. For stronger security and renewability, all cryptographic computations are performed inside tamper-resistant hardware modules. If a cryptographic algorithm or key needs modification, only removable modules, or “cards,” need to be replaced. Importantly, renewability does not impact deployed devices, only their associated cards. Thus, consumers will never have to change their **SmartRight** devices after a lethal hack.

4.7 Revocation

Some attacks may compromise only individual devices, thus not requiring renewability. In such cases, **SmartRight** implements a three-level revocation mechanism:

- Revocation of a PPN: All the devices of the revoked PPN will not be able to handle **SmartRight** content.
- Revocation of a specific smart card: The other security modules will not collaborate with the revoked device.
- Revocation of a display device: Terminal modules will not provide information to a revoked display device.

The revocation mechanism lists revoked entities. The **SmartRight** Association defines, generates, and authenticates these lists. Content carries these lists. An index in content mandates that **SmartRight** devices recognize the latest revocation lists. This “freshness” requirement defeats typical filtering attacks.

4.8 Interoperability

The **SmartRight** system is interoperable on multiple levels, and can operate independently or beside or on top of other digital broadcast (and other) content protections systems. Specifically, **SmartRight** will secure content: alongside competing FCC-approved Broadcast Flag technologies; received via alternative delivery platforms (*e.g.*, cable, direct broadcast satellite, telco/broadband), or any other digital signalling network with access to the home; and on pre-recorded media (*e.g.*, DVDs).

Importantly, consumers with a **SmartRight** PPN will not lose the functionality of their legacy analog equipment, which will be able to receive digital broadcast content by means of a **SmartRight** set-top box.

Finally, **SmartRight** is agnostic with regard to two-way buses (IP, WiFi, Firewire, USB, etc.) and supports multimedia formats such as MPEG-2, MPEG-4 or mp3Pro, etc.

5 Level of Security Provided

5.1 SmartRight Personal Private Network

The **SmartRight** Personal Private Network (PPN) is composed of **SmartRight** devices belonging to the same family (*i.e.*, an authorized digital network). The **SmartRight** PPN consists of at least one Reception Device and a limited number of Display Devices, where all the “Terminal Modules” (each of which resides in a Display Device) contain a unique common “network key.” Although the size of a PPN is limited (but only with regard to display devices; the PPN may include an unlimited number of reception and storage devices), it will accommodate the normal use of consumers within their authorized local or remote network domain (within acceptable proximity constraints, as discussed below).

An important attribute of the **SmartRight** PPN for consumers is that “private-copy” content can be distributed and viewed within the same PPN without any restriction. It can even be recorded, again without restriction, within the same PPN. However, if this recorded content is distributed outside the PPN, such as would be the case if indiscriminately redistributed over the Internet, the content is essentially useless to all other networks.

5.2 End-to-End Protection

The main feature of the **SmartRight** system is end-to-end content protection. The **SmartRight** system achieves end-to-end content protection in the following manner:

- A **SmartRight** reception device controlling access for content that is not already scrambled (*i.e.*, that which would be used for over-the-air content) detects the presence of the Broadcast Flag and scrambles the content using Triple DES. The reception device associates LECM to content before sending it to the home network.
- To render content displayable, the Terminal Module decrypts LECM. If suitable, the Terminal Module securely transmits the control words—*i.e.*, the descrambling key—to the display device. The display device descrambles the content.

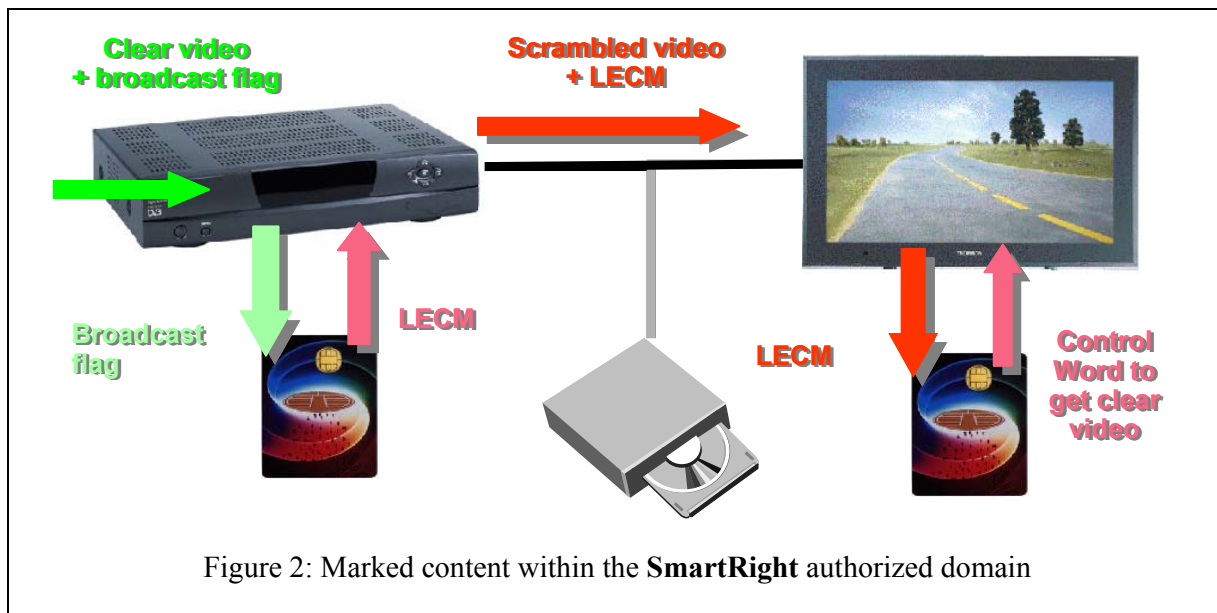


Figure 2: Marked content within the **SmartRight** authorized domain

Figure 2 illustrates the treatment of marked content.

5.3 Preventing Indiscriminate Redistribution Over The Internet

As discussed above, the **SmartRight** content protection system secures digital broadcast content within a seamless network of authorized devices, the Personal Private Network. Once received, **SmartRight**-protected content can only be redistributed over the Internet with **SmartRight** redistribution control protection, which effectively renders that content unviewable to any recipient outside the originating Personal Private Network (*i.e.*, including those with a different **SmartRight** Personal Private Network).

The Terminal Modules of devices on a **SmartRight** PPN share the same network key. The first installed Terminal Module generates a random network key. The network key is securely transmitted to each new installed Terminal Module. At a given time, only one Terminal Module is able to transmit the network key to another Terminal Module.

SmartRight limits the number of display devices to a reasonably-defined number that may join the PPN. Once that limit is reached, no new display device can join. The count is done when transferring the network key to a new Terminal Module. There is no limitation on the number of devices with reception or storage capability that can be attached to the PPN.

5.4 Proximity Control

SmartRight allows the consumer to include within his or her PPN remotely-located devices, such as those in a second home, office, car or boat. The transfer of content between the remote locations may be either via physical storage media or via the Internet – in each instance with **SmartRight** protection applied. Recognizing that the latter case may implicate content owners' rights vis-à-vis secondary and foreign markets (*e.g.*, content broadcast in New York City should

not concurrently be available for viewing in Paris), the **SmartRight** system offers Proximity Control: a means to control the transfer over the Internet of **SmartRight**-protected content between remote locations within the same PPN, based upon the geographic proximity of those locations. If activated, Proximity Control – using a balanced analysis of the number of routers, and the latency time of communication – will block the transfer of protected content over a Wide Area Network, based upon parameters acceptable to the owners of the specific content being transferred. In any case, the same **SmartRight**-protected content may be transferred between those remote locations through a **SmartRight**-protected physical storage media, such as a recordable DVD.

5.5 Local Enforcement Copy-Management Message

The **SmartRight** system's protected data structure, called the Local Enforcement Copy-Management Message (LECM), contains two parts: the clear section and the protected section. The latter section carries the control word, i.e. the descrambling key. The protected section is encrypted for "Private Copy" content. In the case of "copy freely," the protected section is in the clear (plaintext).

The LECM carries information such as:

- Broadcast Flag
- **SmartRight** usage states
- Output Control Information defining the rules of exportation
- The value of the LECM key encrypted by the network key
- Control words

The Converter Module picks at random the LECM key. The Converter Module asks one of the network Terminal Modules to encrypt that LECM key with the network key. For that purpose, the Converter Module sends the LECM key encrypted with the public key of the Terminal Module. The Terminal Module encrypts the received LECM key with the network key. It returns the encrypted LECM key to the Converter Module.

The Converter Module encrypts the protected part of the LECM with the LECM key. It adds the encrypted LECM key to the clear part of LECM. When receiving a LECM, the Terminal Module decrypts the encrypted LECM key with its network key. It then decrypts the protected part of LECM with the LECM key. It now has access to the control words.

5.6 Enforcement of Usage Rights

With respect to DTV content, the **SmartRight** system supports two usage states: "Copy Freely" and "Private-Copy." Enforcement of these states is accomplished in the following manner:

5.6.1 Copy Freely

Content that does not have the presence of the Broadcast Flag will be marked "Copy Freely" and may be freely copied by the consumer and redistributed to other **SmartRight** PPNs for viewing or storing. Although the content is scrambled, the LECM is in the clear. Thus, any Terminal Module, even from another PPN, can provide the control words to descramble the content.

5.6.2 Private Copy

Content that has the presence of the Broadcast Flag will be marked “Private Copy” and may be freely copied by the consumer within his or her PPN but cannot be redistributed, either to other **SmartRight** PPNs or over the Internet, in a viewable manner. “Private-copy” content can only be viewed within the PPN where it has been created.

The protected part of the LECM is encrypted with the LECM key. The clear part of the LECM holds the LECM key encrypted with the network key. Thus, any Terminal Module belonging to this PPN can decrypt the encrypted LECM key. It then decrypts the protected part of LECM. It can provide the control words to descramble the content. A Terminal Module belonging to another PPN does not have the right network key to access the LECM key.

5.7 Security analysis

5.7.1 Trust Model

The **SmartRight** system relies mainly on two secrets and one security assumption, as follows:

- A global secret: the private key used to sign the certificates and revocation lists. This 2048-bit private key will be in one unique location and protected with the strictest security policy.
- An individual secret: the 128-bit network key that is unique to every PPN. This secret is stored inside tamperproof hardware - the terminal card. It leaves this safe environment only when transferred to another terminal card. The transfer uses a typical secure exchange.
- The behavior of the terminal card follows the specifications.


To enforce the two last conditions, a **SmartRight** system uses tamperproof modules for Terminal Modules. Hardware tamper resistance ensures the secrecy of the network key and a trustful behavior. The compliance rules of a terminal card are defined using a dedicated Protection Profile of Common Criteria. The target level is EAL4+. (Notably, this requested level dramatically exceeds the security afforded by current Pay TV cards).

These three requirements compose the kernel of the security model of **SmartRight**. Nevertheless, as discussed further below, many “second fences” have been added, such as © watermark, revocation, and ultimately full system renewability by card replacement.

5.7.2 Security Mechanisms

SmartRight uses many different security mechanisms. Following is a non-exhaustive list of these mechanisms:

- **SmartRight** modules mutually authenticate each other. The presence of a module that will fail authentication blocks the exchange of content within a PPN. Furthermore, removable **SmartRight** modules authenticate their host device. The use of certified keys safeguards against forged new **SmartRight** modules. Unauthorized users may only create clone cards. Revocation answers this threat.

-
- 
- Content always remains scrambled within a Personal Private Network. Descrambling occurs only at the display. Thus, it is useless for the unauthorized user to wiretap content.
 - Descrambling keys are protected with Advance Encryption Standard (AES) and with a key unique to a Personal Private Network. Thus, two Personal Private Networks cannot exchange **SmartRight** protected content.
 - Copyright watermark detection (see Section 5.8) spots illegal content that would have leaked, for instance, through an “analog hole,” or DeCSS like software.
 - A patented mechanism limits the size of the Personal Private Network, i.e. the number of display devices. Furthermore, this mechanism prevents the use of peer-to-peer networks to set up an illegal Personal Private Network.
 - Through the mandatory use of Common Criteria evaluation, hardware tamper resistant modules ensure secrecy of the keys and provide a secure execution environment.

5.7.3 Protocols

All the designed protocols have been carefully crypto analyzed by the security specialists of each company, especially AXALTO, GEMPLUS and NAGRAVISION. The specialists analyzing the protocols were not members of the design team. Furthermore, the protocols have been crypto analyzed by an external, world renowned, expert, Jacques Stern.


5.7.4 Proposed Algorithms

The **SmartRight** system uses only state of the art published algorithms:

- Content is scrambled using Triple (DES) with 112 bit-length keys as defined in FIPS 46-3.
- LECMs are encrypted using AES with 128 bit-length keys as defined in FIPS-197.
- Asymmetric encryption uses RSA with 1024 certified bit-length keys as defined by PKCS#1 version 2.1.
- Authentication uses RSA. The root key for certification uses RSA with 2048 bit-length keys.
- Hash uses SHA-1.

5.8 Copyright Watermark

The **SmartRight** system offers an additional optional security mechanism. Broadcasters or content providers can add a **SmartRight** dedicated watermark, the so-called Copyright © watermark (which carries no payload), to indicate that the content should be protected, and thus scrambled. Within a **SmartRight** PPN, © watermarked content must be scrambled. When a **SmartRight** display encounters content carrying a clear © watermark content, it considers the content illegal and stops rendering.



Due to its null payload, the © watermark is inherently more robust than any scheme using a payload. In other words, it will be more difficult to “wash” the © watermark.

SmartRight’s innovative use of watermarking offers broadcasters and content owners a powerful tool with which to combat the “analog hole,” thus even more effectively preventing unauthorized indiscriminate Internet redistribution of their high-value digital content.

6 Renewability and Revocation

6.1 Protection Against Circumvention Devices

The **SmartRight** system protects against the following types of attacks:

- Clone Terminal Modules.
- Fake terminal cards using a regular certificate. Signature of the **SmartRight** certification authority prevents forging new certificates.
- Rogue host devices with tampered copy protection means (*e.g.*, with digital output copy protection disabled).
- Large-scale impersonation of a host device by a PC.
- Crackers having retrieved one network key and making use of it (*e.g.*, distribution of content in-the-clear).

6.2 Renewability And Resistance To Obsolescence

Removable security modules, or “smart cards,” ensure full renewability of the **SmartRight** system. In the event the system is “hacked,” or when the system needs an upgrade, a new version of the smart cards is issued to the consumer, who is able to install the cards quickly and easily.


Version control numbers attached to content indicate the minimum requested version for converter cards and terminal cards. The modules check these data and inform their respective host devices of the need for newer cards. After a short-term transition phase, all new content will carry the newer version number. Obsolete modules cannot process new content. Nevertheless, obsolete modules can still process content stored with older versions.

All decisions relating to **SmartRight** renewability are based upon an assessment of the attack by the **SmartRight** Association.

6.3 Revocation

The **SmartRight** system supports three types of revocation:

- **Revocation of Terminal Module:** Once a terminal certificate is revoked, no pirate terminal cards using this certificate will be granted access to a **SmartRight** PPN. Every **SmartRight** module will refuse to collaborate with revoked Terminal Modules. This type of revocation occurs if more than one Terminal Module holds the same unique identifier.
- **Revocation of Display:** Once a display’s certificate is revoked, every Terminal Module refuses to collaborate with the revoked display. The Terminal Module does not return the



control words. Nevertheless, other functions of the display are not affected. Revoked displays may play non **SmartRight**–protected content. This type of revocation occurs if more than one display device holds the same unique identifier; and

- **Revocation of an Entire PPN:** Once a network key is revoked, compliant modules will stop operating with that network key. This type of revocation occurs if a network key is present in more than the maximum authorized number of Terminal Modules.

7 Interoperability

The **SmartRight** system has a broad portfolio of interoperability, and is capable of operating either independently as a self-contained system, or beside or on top of other content protection systems. Specifically, **SmartRight** is compatible and/or interoperable with:

- **Other FCC-Approved Broadcast Flag Technologies:** **SmartRight** will receive digital broadcast content protected by other Broadcast Flag protection systems, as well as export content to other copy protection systems. **SmartRight** always preserves the Broadcast Flag for export to other approved digital broadcast content protection systems.
- **Non-Broadcast Delivery Systems:** The protection afforded by **SmartRight** is delivery platform-neutral – in addition to over-the-air delivery, it will secure content received via cable, direct broadcast satellite, telco (such as broadband-delivered), or any other digital signalling network with access to the home. **SmartRight** also is agnostic with regard to potentially different business models.
- **Pre-Recorded Media:** **SmartRight** will secure pre-recorded media.
- **Legacy Equipment:** Especially important to consumers, legacy TV sets will be fully functional alongside a **SmartRight** PPN, and accessed through the use of a **SmartRight** set-top-box utilizing existing analog links, or DVI. Content distributed to these devices will be protected by Macrovision, or DVI-HDCP.
- **Other:** **SmartRight** is not dependent upon any specific interface (IP, WiFi, Firewire, USB, etc.). In addition to MPEG-2, the **SmartRight** system supports other multimedia formats such as MPEG-4 or mp3Pro, etc.

8 Consumer Use and Enjoyment

While the goal of the Broadcast Flag is the protection of digital broadcast content from indiscriminate redistribution over the Internet, it should be accomplished only in a manner that preserves consumers' use and enjoyment of over-the-air broadcast content, lest the DTV transition be rejected by consumers as a "step backwards" from what they have today. Ensuring that the DTV experience is one that consumers will embrace wholeheartedly is a core principle of the **SmartRight** system.

8.1 SmartRight Preserves The "Freely-Copiable" Environment

SmartRight entirely preserves, in the digital content realm, the "copy freely" environment consumers enjoy today with analog broadcast content. Within a **SmartRight** Personal Private Network, consumers will be able to copy – both with respect to non-removable storage media (*i.e.*, hard drives) and removable storage media (*i.e.*, recordable DVDs) – marked and unmarked DTV content and then view that content on any display device within the Personal Private Network.

8.2 SmartRight Enhances Consumers' Use and Enjoyment of DTV By Permitting Secure, *Discriminating* Internet Redistribution of Protected DTV Content To A Second Home, Car, Boat or Office

In addition to permitting access and enjoyment of protected digital broadcast content within the traditional confines of a local domain of authorized devices (*i.e.*, those within a single home), **SmartRight** allows the consumer to expand his/her PPN to include a remote domain, such as a car, second home, office, portable devices or boat, and to send **SmartRight**-protected content to those devices over the Internet in a secure and discriminating fashion. Moreover, from a consumer's perspective, joining a device to an existing PPN, or even creating a new PPN, is hassle-free. There is no need to connect the device to a "back office" via the Internet or dialup for registration, which means that the user has no need to disclose and expose any personal information. The process is completely transparent to the consumer.

8.3 SmartRight Preserves the Functionality of Legacy Devices

The **SmartRight** system in no way diminishes the functionality of legacy analog devices. Such devices will be able to send and receive digital broadcast content over the **SmartRight** Personal Private Network through the use of a separate **SmartRight** set-top box.

9 The SmartRight License

9.1 Overview

SmartRight will be licensed on a reasonable and non-discriminatory basis.³ The **SmartRight** license contains a number of unique provisions which are designed to accommodate the rights of the public to fairly use digital broadcast content within their Personal Private Network, protect the legitimate interests of equipment manufacturers as well as to provide content providers with a robust system that will provide outstanding protection against unauthorized redistribution of their works. Some examples of such provisions include:

- Implementation of a Personal Private Network that permits consumers to display content received by them on a variety of devices both within their homes and elsewhere, while still preventing unauthorized indiscriminate dissemination over the Internet and outside of the user's personal network.
- Provision for full compatibility with other content protection systems, so that consumers will not lose the use of legacy devices or the ability to view content on non-**SmartRight** devices that provide alternative means of approved protection.
- The ability to revoke individual keys coupled with procedural protections to protect consumers against unfair or erroneous use of that capability;
- A renewal process which permits a general replacement of any compromised technology without adversely affecting the interests of consumers;
- Limitations on changes to the specification and compliance rules that would adversely impact equipment manufacturers and procedural protections for adopters to safeguard competition, patterned after the DFAST license used in connection with unidirectional digital cable-ready products;
- The granting of an option to adopters who have essential patents to preserve their intellectual property rights subject only to an obligation to license their fellow adopters on reasonable and non-discriminatory terms, again, consistent with the approach taken in the DFAST license;
- A qualification procedure which permits manufacturers to self-certify their products as compliant while preserving overall supervision and quality control;
- The granting of express third party rights to digital broadcast content providers to enforce the agreement;
- Full potential for the implementation of an analog watermark protection system.

³ As noted above, the **SmartRight** License Agreement is attached as Appendix A.

-
- Compliance rules that are specifically tailored to the particular requirements of publicly disseminated broadcast content, while still affording a broad range of protection to commercial audio-visual content originating from a wide variety of other services and media.
 - Robustness rules that conform to the FCC’s “ordinary user” standard.

9.2 Structure of Agreement

The Agreement is divided into four main sections: (i) a license setting out the legal rights and obligation of the parties; (ii) a set of procedural rules, including the current fee structure as well as the procedures applicable to revocation and renewal and third party enforcement of the agreement; (iii) a detailed set of compliance rules specifying the rights and restrictions imposed on each of the four categories of **SmartRight** products for output, storage and recording of marked broadcast content as well as the various types of conditional access content protectable by the **SmartRight** System and (iv) a set of robustness rules designed to assure that all **SmartRight** Products cannot be defeated or circumvented by an ordinary user using generally available tools and equipment.

9.3 Fees

The License is structured initially as an evaluation license for an annual fee of \$10,000. Upon payment of a \$30,000 fee, the license can be converted to a full production license with broad rights to **SmartRight** proprietary technology, including essential patents, to make, have made, use, import, offer to sell and sell **SmartRight** products, along with a trademark and copyright license. In addition, producers of finished products will be required to pay a per unit royalty and certified key fee. Reasonable charges would also be imposed to compensate the Licensing Authority for the costs of preparing and certifying keys, providing reference modules for adopters who wish to acquire them and for qualification of devices for adopters who do not wish to employ the self-qualification option. The overall cost of **SmartRight** implementation – including hardware, software and licensing costs – is comparable to other digital broadcast content protection technologies that have been deployed in the market.

9.4 Reciprocal Licensing

SmartRight Adopters holding essential patent claims will have the option to agree either not to assert those claims against fellow adopters or to make licenses available to those Adopters on reasonable and non-discriminatory terms.

9.5 Approval Process

The **SmartRight** License provides two alternative mechanisms for qualifying licensed products: (i) a “self-test” procedure under which the products will be tested in accordance with a qualification test-suite prepared by the licensing authority, and test results are submitted for verification and review to the Licensing Authority along with other documentation or (ii) inspection and testing by the Authority upon payment of a reasonable and non-discriminatory fee.

9.6 Confidentiality

The license includes strict controls to preserve confidential information. Certain types of information, including Certified Keys, are deemed “Highly Confidential Information” and are subject to highly stringent protections, including a prohibition against copying.

9.7 Changes

The agreement does not permit material changes to the specification or the compliance rules, which would materially increase the cost or complexity of **SmartRight** products, the sole exception being changes mandated by the FCC or other governmental authority. It provides for notification of changes to adopters, opportunity to resolve objections, arbitration to resolve disputes, and a reasonable period in which to implement changes. The **SmartRight** System is designed so that certain changes to existing devices can be implemented through the use of Smart Cards.

9.8 Term and Termination

The license is terminable by adopters on 90 days notice, but can only be terminated by the Authority for material or repeated uncured breaches by the adopter.

9.9 Disclaimer And Limitation of Liability

The license contains typical disclaimers of warranties and limitations of damages. In all events damages are limited to one year’s total payments under the agreement.

9.10 Remedies

Remedies against adopters who breach the agreement include indemnification of the Authority, equitable relief, including specific performance or injunctive relief, and, if a material breach results in the compromise of confidential information, possible liquidated damages of \$1 million. In addition to the Authority, publishers of marked content, content participants and fellow adopters are expressly granted the right to enforce the agreement as third party beneficiaries.

9.11 Revocation and Renewal

The License takes advantage of the ability of the **SmartRight** system to render useless the keys in existing devices and to replace them through the use of removable modules, or “Smart Cards,” by providing for revocation of individual keys which have been compromised as well as the large scale replacement of existing keys and other elements of the system through the renewal procedure. The decision to implement revocation or renewal is vested in the **SmartRight** Association, a not for profit corporation which represents the interests of content providers and adopters. Affected consumers will have the right to challenge and seek judicial review of revocation decisions. The Association will be responsible for affecting renewal at no cost to consumers.

9.12 Compliance Rules Applicable to Unencrypted Digital Broadcast Content

In general, all **SmartRight** devices will comply with the compliance rules for unscreened and marked content set forth in 47 C.F.R. §§73.9003 and 73.9004. However, different types of devices will perform different functions in order to take advantage of the end-to-end protection afforded by the system. Thus, acquisition devices will screen the content for the Broadcast Flag and designate unmarked content as “copy freely” and marked content as “private copy.” Based on that designation, marked content can be viewed on display devices on the user’s Personal Private Network, but will not be permitted to be displayed or decrypted outside of the network. In addition, proximity rules will restrict, on a geographic basis, distribution of even encrypted content over the Internet. Display devices which decrypt the content will preserve the Broadcast Flag and will only permit digital output of decrypted content to approved devices capable of responding to the flag. No restrictions are imposed on analog output of broadcast content. However, the rules also require conformity with “view only” and other types of restrictions that are applicable to Conditional Access Content other than Unencrypted Terrestrial Broadcast Content.

9.13 Robustness Rules

The License adopts and implements the robustness standards imposed by 47 C.F.R. §9007, and imposes detailed robustness rules for all licensed devices, data paths, software functions, distributed functions, hardware, smart cards and other elements of the system, and grants the authority a broad inspection right to assure compliance. Consistent with this rule, the license requires that compliant devices be manufactured in a manner so that they cannot be defeated or circumvented merely by an ordinary user using generally-available tools or equipment.

10 Marketplace Support for SmartRight

Although **SmartRight** has not yet been deployed in the marketplace, it enjoys the support of multiple companies leading the way in digital technology innovation – including hardware and software. Many of these companies are expected to participate as members of the **SmartRight** Association. These companies include:

AXALTO, a leading provider of microprocessor cards and a major supplier of point-of-sale terminals. Axalto serves customers in more than 100 countries, with worldwide sales exceeding 2.8 smart cards to date. [<http://www.axalto.com>]

GEMPLUS SA, a leading provider of smart card enabled technology, products and services for secured wireless communications and transactions specializing in the telecommunications (mobile telecom and public telephony) and financial services sector (banking, government and large enterprise, retail, and electronic OEM). [<http://www.gemplus.com>]

MICRONAS, a leading supplier of innovative, application specific microchips (integrated circuits and sensors) primarily for use in the consumer electronics (TV, video, and radio equipment) and automotive industries. [<http://www.micronas.com>]

NAGRAVISION SA, a market leader in the field of conditional access for digital television and broadband Internet. Leading operators are equipped with Nagravision's technology, which ensures secure access to their services via more than 35 million decoders (analog and digital). [From their website: <http://www.nagravision.com>]

PIONEER CORPORATION, a world leader in digital entertainment products and technology advancements in the consumer electronics industry. [<http://www.pioneerelectronics.com>]

SCM MICROSYSTEMS, a leading supplier of Smart Card reading technology for the PC platform and conditional access modules for the digital television platform to OEM customers in government, financial services, enterprise and broadcast markets worldwide. [<http://www.scmicro.com>]

ST MICROELECTRONICS N.V., a leader in developing and delivering semiconductor solutions across the spectrum of microelectronics applications. [<http://www.st.com>]

It is also anticipated that other companies with whom Thomson and the **SmartRight** members are talking (to include content creators and network distributors) will endorse and support **SmartRight** as an acceptable and secure content protection system.

Annex A : Abbreviations

| | |
|------|---|
| DES | Data Encryption Standard |
| DVD | Digital Versatile Disc |
| LECM | Local Enforcement Copy-Management Message |
| NRSS | National Renewability Secure Standard |
| PPN | Personal Private Network |
| STB | Set Top Box |

Table 1: List of used abbreviations



**Certification for FCC Approval
for Use With the Broadcast Flag**

APPENDIX A
SmartRight License Agreement
March 1, 2004



LICENSE AGREEMENT

Evaluation License Convertible to Product License

This SmartRight® License Agreement, (“Agreement”) is effective as of the latest date set out on the signature page hereof (the “Effective Date”) by and between the SmartRight Licensing Authority, LLC, (the “Authority”) and the Adopter named immediately below:

| | |
|---|--|
| Name of Adopter: | |
| Description of Adopter’s Business | |
| Name of Contact Person: | |
| Contact Person’s Address, Phone Fax number E-mail Address: | |
| Location of Principal Office: | |
| Jurisdiction of Adopter’s Formation: | |
| Year of Formation: | |
| Number of Employees: | |
| Amount of Capital: | |

RECITALS

Whereas the Authority is the authorized Licensor of the SmartRight® system for protecting certain digital content from unauthorized use as described in the SmartRight Specification (the "Specification"); and

Whereas Adopter wishes to receive a license, subject to the terms and conditions set forth in this Agreement for the purpose of developing and evaluating and, at its option, implementing SmartRight, in accordance with the terms of this Agreement, including, but not limited to, the Compliance Rules annexed hereto.

Therefore, the Authority and Adopter agree as follows:

TERMS OF AGREEMENT

Article I. DEFINITIONS

In addition to terms defined elsewhere in this Agreement, the following terms shall have the following meanings. All definitions herein shall apply equally to their singular and plural forms, all pronouns shall apply without regard to gender, and all references to Sections and Exhibits shall be deemed to be references to Sections of, and Exhibits to, this Agreement unless the context shall otherwise require.

1.1 **"Acquisition Device"** is defined in the Compliance Rules.

1.2 **"Activation"** means that the Adopter has executed the Activation Notice and has paid the fee referenced in Section 2.3, which is required to activate the Adopter's production license.

1.3 **"Adopter"** means the entity named at the beginning of this Agreement and includes its Affiliates.

1.4 **"Adopter Agreement"** means this Agreement and any other SmartRight License Agreement entered into by the Authority and any other adopter of SmartRight.

1.5 **"Affiliate"** means with respect to any person or entity, any other person or entity directly or indirectly controlling or controlled by or under direct or indirect common control with such person or entity. "Control" means the possession of beneficial ownership of more than 50% of the stock or other similar interest entitled to vote for election of the Board of Directors or similar managing Authority.

1.6 **"Association"** means the SmartRight Association, Inc., a not for profit corporation established to administer the Renewal of SmartRight Products on behalf of content providers, distributors and adopters in conformity with the Procedural Rules.

1.7 **"Certificate"** means a string of data bits attached to a Key for the purpose of identifying and validating the source of the Key.

1.8 **"Certified Key"** means a Key having an attached Certificate.

1.9 **"Combination Device"** is defined in the Compliance Rules.

1.10 **"Commercial Audiovisual Content"** is defined in the Compliance Rules.

1.11 **"Common Criteria"** means ISO/IEC 15408.

1.12 **"Compliance Rules"** means that document of the same name which is hereby incorporated into this Agreement by reference, as may be amended by the Authority from time to time. A Copy of the current Procedural Rules is annexed as Exhibit B to this Agreement.

1.13 **"Compliant"** means conforms in all respects to the Specification, the Compliance Rules and the Robustness Rules.

1.14 **"Conditional Access Content"** has the meaning set forth in the Compliance Rules.

1.15 **"Confidential Information"** means all information disclosed by either party to this Agreement that has been identified or designated to be confidential and proprietary, or that a reasonable person would judge to be confidential under the circumstances, including without limitation, any information concerning unpublished copyrighted works or mask works, unpublished pending patent applications, development materials, source code, unmarketed products or components, design documentation, system documentation specifications, and any information regarding such party's financial, business, and marketing matters. Except as provided in section 7.3.2, Confidential Information includes Highly Confidential Information. A party's status as an Adopter, or lack thereof, shall not be deemed Confidential Information.

1.16 **"Content Participant"** means a party who distributes or transmits, or cause or authorize the distribution or transmission of Conditional Access Content who has entered into an agreement with the Authority authorizing that party to protect its content through the use of the SmartRight System.

1.17 **"Converter Card"** means a SmartRight Smart Card intended for use with an Acquisition Device.

1.18 **"Device Key"** means a unique Certified Key which has been assigned to a particular Finished Licensed Product.

1.19 **"Essential Patent Claims"** means claims of a patent or patent application that would be necessarily and unavoidably infringed by the manufacture, use, sale, offer for sale or import or other disposition of a product in order to comply with the

SmartRight™ Specification in a particular country in the absence of a license or other authorization from the owner of such patent claims in such country. As used herein, "infringe" includes direct infringement, contributory infringement and/or inducement of infringement. Essential Patent Claims shall not include patent claims for a technology that has been developed by third parties independent of the SmartRight System but has been incorporated and referenced in the Specification for use in the SmartRight System.

1.20 **"Fellow Adopters"** means any entity other than the Adopter which has executed an Adopter Agreement and delivered it to the Authority or its designee.

1.21 **"Finished Licensed Product"** means an Acquisition Device, Presentation Device, Combination Device, Storage Only Device, Converter Card, or Terminal Card in a form that is intended to be distributed directly to end-users and which embodies any SmartRight Technology.

1.22 **"Generator"** means the Authority or an entity that has been retained by the Authority to generate Device Certificates and Device Keys for use by Adopters.

1.23 **"Highly Confidential Information"** means Confidential Information of the Authority that is marked or otherwise "Highly Confidential Information" or otherwise designated as such by the Authority. All Certified Keys are Highly Confidential Information.

1.24 **"Key"** means a string of information used by a cryptographic function either to encrypt, decrypt, sign, or check the signature of a message.

1.25 **"Licensed Marks"** means the trademark "SmartRight" in all jurisdictions in which it has been registered or adopted by the Authority and any other trademarks which the Authority by register or adopt for use in connection with Licensed Products.

1.26 **"Licensed Patents"** means all Essential Patent Claims of the patents and applications which the Authority has been authorized to license.

1.27 **"Licensed Product"** means a Finished License Product or a Licensed Component.

1.28 **"Licensed Component"** means a product, such as an integrated circuit, circuit board, or software module, that is designed to be incorporated into a Licensed Product and that embodies any SmartRight Technology.

1.29 **"Licensed Technology"** means the Licensed Patents, the Specification and all trade secrets, copyrights, mask rights and other exclusive rights which relate thereto and which the Authority owns or is authorized to license other than the Licensed Marks.

1.30 **“Local Enforcement Copy-Management Message” or “LECM”** means a data structure defined in the Specification which includes the Key necessary to decrypt SmartRight content and designates the content as “Copy Freely”, “View Only” or “Private Copy.”

1.31 **“Marked Content”** has meaning set forth in the Compliance Rules.

1.32 **“Maximum Network Size”** means the maximum number of terminal modules permitted to share the same Network Key on a PPN.

1.33 **“Network Key”** means a Key generated by a Terminal Module and used by all Terminal Modules on a PPN to decrypt an LECM created by a converter module associated with that PPN.

1.34 **“Party”** means the Authority or the Adopter.

1.35 **“Personal Private Network” or “PPN”** means a plurality of devices designed for the acquisition, storage, transmission, recording, reproduction and/or presentation of Commercial Audiovisual Content owned by the members of a single household and intended for use solely by the members of that household.

1.36 **“Presentation Device”** is defined in the compliance rules.

1.37 **“Procedural Rules”** means that document of the same name which is hereby incorporated into this Agreement by reference, as may be amended by the Authority from time to time. A Copy of the current Procedural Rules is annexed as Exhibit A to this Agreement.

1.38 **“Registered Owners”** means end-users who have purchased SmartRight Products and who have provided the Adopter with information sufficient to permit communications to be addressed to such person.

1.39 **“Renewal”** has the meaning ascribed in Section 4.1.

1.40 **“Renewal Criteria”** means those criteria for Renewal set forth in Section 4.3.

1.41 **“Revocation”** has the meaning ascribed in Section 4.1.

1.42 **“Revocation Criteria”** means those criteria for Revocation set forth in Section 4.2.

1.43 **“Rights”** means the Licensed Patents, the Licensed Technology and the Licensed Marks.

1.44 **“Robustness Rules”** means that document of the same name which is hereby incorporated into this Agreement by reference, as may be amended by

the Authority from time to time. A Copy of the current Procedural Rules is annexed as Exhibit C to this Agreement.

1.45 **“SmartRight Content”** means content that has been encrypted and packaged with a Local Enforcement Copy-Management Message ("LECM") in accordance with the SmartRight Specification. SmartRight Content includes Encrypted SmartRight Content and Decrypted SmartRight content.

1.46 **“SmartRight Label”** means a holographic sticker or label issued by the Authority to be affixed to SmartRight Products for which a per unit license fee has been paid.

1.47 **“SmartRight Products”** means Compliant Finished Licensed Finished Products that have been qualified pursuant to sections 6.3 or 6.4. SmartRight Products may be Acquisition Devices, Presentation Devices or both.

1.48 **“Smart Card”** means either a Converter Card or a Terminal Card.

1.49 **“SmartRight Smart Cards”** means Smart Cards that are Qualified pursuant to section 7.2. A Smart Right Smart Card may function as a Converter Card, a Terminal Card or both.

1.50 **“Specification”** means the specification entitled “SmartRight Specification” issued by the Authority, as may be amended from time to time pursuant to Section 3.3.

1.51 **“Terminal Card”** means a SmartRight Smart Card intended for use in a Presentation Device.

1.52 **“Terminal Module”** means a Terminal Card or an integrated module in a Presentation Device which performs the functions of a Terminal Card.

Article II. FEES

2.1 **Current Fees and Modifications.** The Fees currently chargeable by the Authority to Adopters are set out in Procedural Rules. The Authority may, upon at least thirty (30) days notice to Adopter, modify the Annual Administration Fee and Certificate Fees payable for the period beginning on the next Annual Payment Date, provided that any increase in such fees shall not exceed an amount commensurate with any increase in the Authority's costs (including but not limited to the cost of inflation). Without limiting the foregoing, where costs per Certificate or per Adopter decrease, the Authority shall use commercially reasonable efforts to reduce the Per Certificate Fee or Annual Administration Fee, respectively.

2.2 **Annual Administration Fee, Evaluation Rights.** Within thirty (30) days of the Effective Date, Adopter shall pay the Authority a nonrefundable sum in the amount of the Annual Administration Fee for Evaluation Rights set out in the Proce-

dural Rules (the Adopter shall not be entitled to any refund thereof for any reason. Upon each anniversary of the Effective Date (the “Annual Payment Date”), or such other date as specified in the Procedural Rules, Adopter shall pay the Authority the Annual Administration Fee for the following year,

2.3 Annual Administration Fee, Production Rights. At any time following the Effective Date, Adopter may Activate the Production License granted under section 5.2 by payment of an Annual Administrative Fee for Production Rights in the amount set forth in the Procedural Rules and submitting of an Activation Notice in the form promulgated by the Authority. To the extent the Adopter has previously paid a fee for Evaluation Rights for the then current year, a pro-rated portion of such fee for the period remaining until the next Annual Payment Date shall be credited against its Annual Administrative Fee for Production Rights. Following Activation, the Adopter’s Annual Payment Date shall be the anniversary date of its initial Activation, or such other date as specified in the Procedural Rules.

2.4 Certified Key Fees. Certified Device Keys are necessary to manufacture some Licensed Products. Certified Device Keys are generated by the Generator under the direction of the Authority. Following Activation, Certified Device Keys shall be made available according to the fee schedule set out in the Procedural Rules, as updated from time to time in accordance with the terms of this Agreement. Prior to Activation, Facsimile Certified Device Keys shall be issued to Adopter for development purposes only. Such facsimile Certified Devices Keys will not inter-operate with commercial devices and Devices which incorporate facsimile Certified Keys will not be deemed Licensed Products within the meaning of this Agreement.

2.5 Per Unit Royalty. In addition to the Annual Administrative Fee, set forth in section 2.3, above, Adopter will pay a royalty fee of \$2.00 per unit in advance for each SmartRight Product sold by Adopter. Upon receipt of such payment, the Authority will issue a SmartRight Label to be affixed by the Adopter to each product prior to sale to authenticate that a per unit royalty has been paid with respect to that product.

2.6 Reference Implementations. The Authority will make reference implementation components available to Adopter for inclusion in Acquisition and Presentation Devices in return for fees as specified in the Procedural Rules.

2.7 Manner of Payment. All fees shall be paid to the Authority or to its order in United States dollars by wire transfer or such other means as the Authority may reasonably specify. Adopter shall be responsible for payments of any taxes or charges imposed the Authority by reason of such fees. If Adopter is required by law to make any withholding from fees due to the Authority, it may make such withholding but shall provide the Authority, at the time of payment, with evidence of such withholding adequate to permit the Authority or its assignee to claim the relevant credit for the amounts withheld.

Article III.
SPECIFICATION AND COMPLIANCE RULES

3.1 **Delivery.** Upon Adopter's execution hereof and the Authority's receipt of the Administration and Disclosure Fee, the Authority shall cause to be distributed to Adopter the relevant portions of the Specification that Adopter has not previously received.

3.2 **Distribution.** Adopter agrees to provide copies of the Specification and Compliance Rules to those persons having supervisory responsibility for the design and manufacture of Licensed Products and Licensed Components for and on behalf of Adopter, in such manner and at such times as to promote Adopter's compliance with all applicable terms thereof.

3.3 **Changes.**

3.3.1 The Specification and the Compliance Rules may be amended from time to time by the Authority only in accordance with this Section 3.3. Adopter shall be required to comply with all amendments to the Compliance Rules and the Specification within eighteen months after the later of (a) delivery of a notice to the Adopter and interested Content Participants of such change in accordance with section 11.7 or (b) the issuance of an award in an arbitration pursuant to section 3.3.4(b). Changes in the Procedural Rules, with the exception of the Annual Administration Fees and Certified Key Fees, shall be effective on no less than thirty days' notice. Changes to the Annual Administration Fees or Certified Key Fees shall be permitted only as set out in Section 2.1. Changes in Per Unit Royalties shall be effective on no less than one years' notice.

3.3.2 The Authority shall not make any material changes to the Specification (including any changes that would expand the Specification to require new technical features not included in the version of the Specification in effect as of the Effective Date that cannot be implemented by the issuance of new Smart Cards or would otherwise create compatibility problems with Licensed Products manufactured prior to such changes); provided, however, that the Authority may make such limited changes, if any, in the Specification as would permit SmartRight to be used with transports other than those permitted in the version of the Specification as may be in effect as of the Effective Date. Without limiting the foregoing, the Authority reserves the right to correct any errors or omissions in the Specification or to make changes that would clarify, but not materially amend, alter or expand the Specification, from time to time.

3.3.3 Except as the Authority may conclude is necessary to comply with regulations of the FCC or other applicable governmental authority, the Authority shall not make any revisions to the Compliance Rules that would materially increase the cost or complexity of implementations of SmartRight Licensed Products.

3.3.4 In the event Adopter, together with one unaffiliated Fellow Adopter notifies the Authority within sixty days after receiving notice of the change,

that it has a bona fide objection to the change on the grounds specified in sections 3.3.2 or 3.3.3, then the following procedures shall apply:

(a) The Authority, interested Content Participants, and the Adopters shall attempt in good faith to resolve the objections to the proposed change during the sixty day period following the delivery of the notice of the objections.

(b) At any time during such sixty day period, any Adopters who have filed timely objections may request arbitration to resolve the dispute by sending to the Authority a notice of intention to arbitrate in accordance with the commercial arbitration rules of the American Arbitration Association (the "Rules"). The parties shall thereafter proceed to arbitrate the dispute before a single arbitrator in the City of New York under the expedited procedures set forth in the Rules, except that the arbitrator shall render his or her award no later than 180 days following the commencement of the arbitration.

Article IV.

REVOCATION AND RENEWAL

4.1 **Generally.** The Specification includes means by which Keys may be invalidated (generally, "Revocation" or "Revoke"). SmartRight Smart Cards and all attributes of SmartRight Products capable of being modified by a Smart Card may also be replaced or modified through the distribution of new SmartRight Smart Cards (generally, "Renewal" or "Renew"). By entering into this agreement, the Adopter hereby consents to grant to the SmartRight Association, Inc. (the "Association"), the right to determine whether any or all Certified Keys issued to the Adopter may be Revoked or SmartRight Products Renewed in accordance with this Article IV and the procedures set forth in the Procedural Rules.

4.2 **Revocation.** The Association may Revoke a Key when it is required to do so pursuant to Section 4.2.4 or it has otherwise been determined, pursuant to the procedures set forth in the Procedural Rules, that one or more of the Revocation Criteria have been satisfied. The "Revocation Criteria" mean the following:

4.2.1 A Device Key has been copied such that the same Key is found in more than one device or product;

4.2.2 A Key has been lost, stolen, intercepted or otherwise misdirected, or made public or disclosed; or

4.2.3 A Network Key is present in more Terminal Modules than permitted by the Maximum Network Size.

4.2.4 The Association is required to revoke a Key by court order, or other competent government Authority.

4.3 **Renewal.** The Association may Renew any or all outstanding SmartRight Smart Cards when it is required to do so pursuant to Section 4.3.3 or it has

otherwise been determined, pursuant to the procedures set forth in the Procedural Rules, that one or more of the Renewal Criteria have been satisfied. The "Renewal Criteria" mean the criteria set forth in Sections 4.3.1, 4.3.2 or 4.3.3:

4.3.1 The Association determines that unauthorized use or distribution of SmartRight content have reached a sufficient level to justify the cost of Renewal.

4.3.2 The Association determines that it is feasible and desirable to upgrade the reliability and security of the SmartRight Technology.

4.3.3 The Association is required to implement a change in outstanding SmartRight Smart Cards by court order, or other competent government Authority.

4.4 **Procedure.** The procedures set out in the Procedural Rules shall govern Revocation and Renewal. Such procedures provide for notice and review of the Authority decisions and/or actions regarding Revocation where requested.

Article V. **LICENSES.**

5.1 **Evaluation License.** Upon execution of this Agreement, and so long as it remains in effect, Authority grants to Adopter (including its Affiliates) a non-exclusive, nontransferable, nonsublicenseable, worldwide license to use the Licensed Technology solely for the purpose of evaluating and developing Licensed Products.

5.2 **Production License.** Upon Activation the Authority grants to Adopter and its affiliates a nonexclusive, nontransferable, nonsublicenseable, worldwide license under the Licensed Technology to make, have made, use, import, offer to sell and sell Licensed Products; provided that such license shall not extend to features of a product that are not required to comply with the Specification, provided, however, that the license to sell granted hereunder shall not apply to the sale of Licensed Finished Products unless (a) a SmartRight Label has been affixed to the product and (b) the Product has been qualified as a SmartRight Product pursuant to section 6.3 or 6.4.

5.3 **Trademark License.** Upon Activation, and subject to the trademark usage guidelines adopted by the Authority, the Authority grants to Adopter (including its Affiliates) a nonexclusive, nontransferable, nonsublicenseable, worldwide license to use the Licensed Marks solely in connection with the sale, distribution and marketing of SmartRight Products that have been qualified pursuant to section 6.3 or 6.4. .

5.4 **Copyright License.** The Authority grants to Adopter and its Affiliates a nonexclusive, nontransferable, worldwide license to reproduce, modify and prepare derivative works based upon any copyrighted works or mask works included in the Licensed Technology solely to the extent reasonably necessary to comply with the Specification and the requirements of this Agreement provided however that the license

granted hereunder shall not apply to Highly Confidential Information except as expressly authorized pursuant to section 7.3.1(c)

5.5 Reciprocal Licensing Agreement. In the event Adopter, now or in the future, owns or controls any Essential Patent Claims, Adopter shall, either (a) not assert such claims against any Fellow Adopters for making, having made, using, importing, offering to sell or selling Licensed Products, (b) offer to license all Fellow Adopters and Affiliates under any Essential Patent Claims owned or controlled by Adopter or its Affiliates on terms that are fair, reasonable and non-discriminatory, the right to make, have made, use, import, offering to sell and sale Licensed Products.

5.6 Proper Use. The licenses granted herein are subject to and conditioned on the requirement that Adopter shall not produce or sell any devices or software where such devices or software are designed to circumvent the Compliance Rules, the Robustness Rules or the effectiveness of the Specification.

Article VI.

DISTRIBUTION AND QUALIFICATION OF PRODUCTS

6.1 Licensed Products Qualified. Qualified SmartRight Products may be disposed of in any commercially reasonable manner.

6.2 Licensed Components. Licensed Components may only be furnished to Fellow Adopters and persons or entities providing products or services to Adopter pursuant to the right under Section 5.2 to “have made” Licensed Products (a “Have Made Party”). Licensed Components (Schedule 2) may only be furnished to Fellow Adopters and Have Made Parties. Adopter shall contractually bind any Have Made Party to sell, distribute or otherwise dispose of Licensed Components furnished by or made for Adopter only to Adopter.

6.3 Qualification of SmartRight Products, Self Test. The Authority will provide each Adopter with self-qualification test-suites. To be qualified as a SmartRight Licensed Finished Product and be allowed to bear the License Mark each model of a proposed SmartRight Licensed Finish Product must be fully Compliant and must successfully pass the tests included in the self-qualification test-suite. Terminal Smart Cards must be compliant with the Common Criteria and successfully pass the ISO/IEC 15408 certification to be qualified as SmartRight Licensed Smart Card. Upon successfully completing the self-qualification test-suite, the Adopter shall notify the Authority of each self-qualified product model and provide the Authority with a completed qualification checklist, including test results, in a form to be provided by the Authority and a copy of the service manual therefor.

6.4 Qualification of SmartRight Products by the Authority. The Authority shall provide a Qualification Service which will perform the tests necessary to qualify SmartRight Licensed Finish Products and SmartRight Cards upon request of the Adopter for a reasonable and non-discriminatory fee. If the Adopter wishes to use this service, a sample of the Device and a copy of its service manual must be submitted to the

Authority or a contractor designated by the Authority for such purpose and such model must be approved as Compliant by the Authority or its designee. SmartRight Smart Cards must be compliant with ISO/IEC 15408, and successfully pass the ISO/IEC 15408 certification to be qualified as SmartRight Licensed Smart Card.

6.5 No Sales of Non-qualified Products. Sale of non-Qualified Finished License Products, or any other devices bearing the Licensed Marks, will constitute a material breach of this Agreement subject to the remedies set forth in Article X in addition to any other remedies as may be available to any party. If any Finished Licensed Products sold by Adopter are determined to be non-Compliant, the Authority may require that Adopter withdraw such products from the market.

6.6 Compliance with Laws, Export. Adopter will comply with all applicable rules and regulations of the United States, Japan, Member States of the European Union, and other countries and jurisdictions, including those relating to the export or re-export of commodities, software and technical data insofar as they relate to the activities under this Agreement. Adopter is aware that commodities, software and technical data provided under this Agreement may be and/or are subject to restrictions under the export control laws and regulations of the United States, Japan, Member States of the European Union and other countries and jurisdictions, as applicable, including but not limited to the U.S. Export Administration Act and the U.S. Export Administration Regulations, any relevant and applicable European Union rules and procedures (including rules and procedures of the Member States of the European Union), and the Japanese Foreign Exchange and Foreign Trade Law, and shall obtain any approval required under such laws and regulations whenever it is necessary for such export or re-export.

Article VII.

CONFIDENTIALITY

7.1 Permitted Uses. A Party who receives Confidential information (the "**Receiving Party**") shall use any Confidential Information (and tangible embodiments of any of the foregoing) disclosed to it by the other Party (the "**Disclosing Party**") solely for purposes of exercising its rights and performing its obligations under this Agreement.

7.2 No Circumvention. During the Confidentiality Period set forth in section 7.9, below. Adopter shall not itself nor assist others in producing any devices or software designed to circumvent the Compliance Rules or the effectiveness of the Specification

7.3 Preservation of Confidentiality.

7.3.1 Highly Confidential Information. Adopter shall maintain the confidentiality of Highly Confidential Information in the following manner:

(a) Adopter shall employ procedures for safeguarding Highly Confidential Information at least as rigorous as Adopter would employ for its

own most highly confidential information, such procedures to include, at a minimum: (1) maintaining on Adopter's premises a secure location in which any and all Highly Confidential Information shall be stored; (2) such secure location shall be accessible only by authorized employees; (3) employees shall sign in and out each time such employees visit such secure location; and (4) when Highly Confidential Information is not in use, such information shall be stored in a locked safe at such secure location. The foregoing procedures shall not apply to Certified Keys embedded in a SmartRight Smart Card.

(b) Adopter may disclose Highly Confidential Information only to (i) the minimum possible number of regular employees of Adopter: (1) who have an absolute need to know such Highly Confidential Information in order to enable Adopter to implement SmartRight Technology in compliance with the Specification; and, (2) who are bound in writing by obligations of confidentiality sufficient to protect the Highly Confidential Information in accordance with the terms of this Agreement; and, (b) Have Made Parties who have entered into an agreement with the Authority consistent with the provisions hereof that authorizes such third party to receive such Highly Confidential Information. Distribution of a SmartRight Smart Card or Presentation Device in which a Certified Key has been embedded shall not constitute disclosure for purposes of this section.

(c) Adopter shall not make any copies of any Highly Confidential Information, except that a single copy of a Certified Key may be made for the purpose of embedding a Certified Key into a single Terminal Module, following which the original copy shall be destroyed.. If reasonably required for purposes of this agreement, Adopter may request additional copies of such information and the Authority may in its sole discretion fulfill any such request.

7.3.2 Other Confidential Information. A Receiving Party may disclose Confidential Information of the Disclosing Party, other than Highly Confidential Information, only to employees and individuals retained as independent contractors subject to confidentiality obligations equivalent to those applicable to it's own employees and contractors who have a reasonable need-to-know and are bound in writing by obligations of confidentiality sufficient to protect the Confidential Information in accordance with the terms of this Agreement. Each Receiving Party shall use the same degree of care, but no less than a reasonable degree of care, to avoid unauthorized disclosure or use of Confidential Information as such party employs with respect to its comparably important confidential information.

7.4 Cooperation and Assistance. Each Party receiving Confidential Information shall make all reasonable efforts to assist the disclosing Party in relation to any claim, action, suit, proceeding, or litigation with respect to any improper or unauthorized use or disclosure of Confidential Information by any present or former employees of the receiving Party or any third parties who have obtained Confidential from it.

7.5 Contact Person. Adopter shall designate a single employee and an alternate employee who shall receive all Confidential Information and Highly Confidential Information (the "Adopter Contact") disclosed by the Authority.

7.6 Notification of Unauthorized Use or Disclosure. Each Party shall notify the other Party in writing immediately upon discovery of any unauthorized use or disclosure of Proprietary Information, and will cooperate with the Authority in every reasonable way to regain possession of Proprietary Information and prevent its further unauthorized use or disclosure.

7.7 Disclosure Required by Law. If a Receiving Party is required by law, regulation or order of a court or other Authority of competent jurisdiction to disclose Confidential Information, such Receiving Party shall promptly notify the Disclosing Party and shall make reasonable efforts to challenge the discloser or secure an appropriate protective order restricting the scope of use and disclosure of the Confidential Information.

7.8 Confidentiality Exceptions. The restrictions contained in this Article VII shall not apply to information that the Receiving Party can demonstrate by documentary evidence: (i) has been generally known to the public through no breach of the Receiving Party's obligations for more than 120 days and the disclosing party has failed to institute reasonable measures to remove it from public availability or enjoin further public disclosure. (ii) was in the possession of the Receiving Party prior to its Disclosure by the Disclosing Party, (iii) was developed by the Receiving Party's employees (whether independently or jointly with others) without having access (whether directly or through any intermediaries) to such Confidential Information and without any breach of its obligations hereunder, or (iii) is or has been disclosed to the Receiving Party by a third party that had developed (whether independently or jointly with others) such information without any access (whether directly or through any intermediaries) to any Confidential Information and without any breach of any such third party's obligations to the Disclosing Party. Notwithstanding the foregoing any Certified Keys provided to the Adopter shall not lose their status as Highly Confidential Information

7.9 Confidentiality Period. The confidentiality obligations set forth herein shall continue until five years after the last commercial use of SmartRight Technology by the Authority or any Fellow Adopter.

Article VIII. TERM/TERMINATION

8.1 Termination. This Agreement shall be effective upon the Effective Date and shall continue until terminated in accordance with any of the following events:

8.1.1 Termination by Adopter. Adopter shall have the right to terminate this Agreement at any time upon 90 days' prior written notice to the Authority.

8.1.2 **Termination for Breach.** In the event that either party (i) materially breaches any of its obligations hereunder, which breach is not cured within 30 days after written notice is given to the breaching party specifying the breach; or (ii) repeatedly breaches any of its obligations hereunder and fails to cure and cease committing such repeated breaches within 30 days after being given written notice specifying the breaches, then the party not in breach may, by giving written notice thereof to the breaching party, terminate this Agreement, upon the expiration of the 30 day period beginning on the date of such notice of termination.

8.2 **Effect of Termination.** Upon termination or expiration of this Agreement, Adopter shall immediately cease use of Certified Keys. Within 30 days after termination or expiration of this Agreement, (i) Adopter shall return such Certified Keys (ii) each party shall return all other Confidential Information to the Authority; or (ii) destroy all Confidential Information in its possession, retaining no copies thereof, and certify such destruction in writing to the Authority. Within 30 days after termination or expiration of this Agreement, Adopter shall discontinue all manufacture, sale, or distribution of SmartRight Licensed Products.

8.3 **Survival.** Following termination of this Agreement for any reason, the following provisions shall survive: Sections 5.5, 5.6 and 6.5 and Articles VII, VIII, IX, X and XI.

Article IX.

DISCLAIMER AND LIMITATION OF LIABILITY

9.1 **Generally.** The following terms limit the ability of the Adopter to recover any damages from the Authority in excess of fees actually paid to the Authority by Adopter during a one year period. These provisions are an essential part of the bargain, without which the Authority would not be willing to enter into this Agreement.

9.2 **Warranty Disclaimer.** ALL INFORMATION, MATERIALS, KEYS, AND CERTIFICATES ARE PROVIDED "AS IS." THE AUTHORITY AND THE MEMBERS AND CERTIFICATION AUTHORITY MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EXPRESSLY DISCLAIM IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION THAT MIGHT ARISE FROM ANY ACTIVITIES OR INFORMATION DISCLOSURES RELATING TO THIS AGREEMENT. THE AUTHORITY FURTHER DISCLAIMS ANY WARRANTY THAT ANY IMPLEMENTATION OF THE SPECIFICATION, IN WHOLE OR IN PART, WILL BE

FREE FROM INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY OR PROPRIETARY RIGHTS.

9.3 **Limitation of Liability.** THE AUTHORITY NOR ITS MEMBERS NOR ANY DIRECTOR, OFFICER, AGENT, MEMBERS, REPRESENTATIVES, EQUIVALENT CORPORATE OFFICIALS, OR EMPLOYEE OF ANY OF THEM ACTING IN THEIR CAPACITIES AS SUCH (COLLECTIVELY, THE "AFFECTED PARTIES") SHALL BE LIABLE TO ADOPTER FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES ARISING OUT OF ANY CAUSE OF ACTION RELATING TO THIS AGREEMENT, OR BASED ON MAKING, USING, SELLING OR IMPORTING ANY PRODUCTS OF ADOPTER THAT IMPLEMENT PROPRIETARY INFORMATION OR SMART-TRIGH TECHNOLOGY, WHETHER UNDER THEORY OF CONTRACT, TORT, INDEMNITY, PRODUCT LIABILITY OR OTHERWISE. TO THE EXTENT THAT ANY COURT OF COMPETENT JURISDICTION RENDERS JUDGMENT AGAINST THE AUTHORITY NOTWITHSTANDING THE ABOVE LIMITATION, THE AFFECTED PARTIES' AGGREGATE LIABILITY TO ADOPTER IN CONNECTION WITH THIS AGREEMENT SHALL IN NO EVENT EXCEED THE AMOUNTS OF MONEY RECEIVED BY THE AUTHORITY FROM ADOPTER UNDER THIS AGREEMENT IN ANY ONE YEAR PERIOD.

Article X. REMEDIES

10.1 **Indemnification for Wrongful Acts of Adopter.** Adopter shall indemnify and hold the Authority, the Members, the Generator, and their officers, members, representatives, agents, directors, equivalent corporate officials, and employees, harmless from and defend against any claims, actions, suits, proceedings or litigation, and any losses, deficiencies, damages, liabilities, costs and expenses including without limitation, reasonable attorneys' fees and all related costs and expenses, to be paid or otherwise incurred in connection with the defense of any claim, action, suit, proceeding or litigation, that arises from any material breach of any covenant, agreement, representation or warranty herein or claimed wrongdoing by the Adopter.

10.2 **Equitable Relief.** The Authority and Adopter agree and acknowledge that, due to the unique nature of certain provisions hereof, the lasting effect of and harm from a breach of such provisions, including the potential for widespread unauthorized distribution of copyrighted content intended to be protected using the Specification, if a Party breaches its obligations hereunder, money damages alone may not adequately compensate an injured party, and that injury to such party may be irreparable, and that specific performance or injunctive relief is an appropriate remedy to prevent further or threatened breaches hereof.

10.3 **Liquidated Damages Measure and Limitation.** The parties agree that it would be difficult to ascertain the amount of damages in the event of certain

breaches of its obligations by adopter and that damages therefor shall be liquidated as follows:

10.3.1 In the event of a material breach by Adopter of the provisions of Article VII, that results in the unauthorized use or disclosure of Confidential Information by a third party, Adopter shall be liable for \$1 million dollars;

10.3.2 In the event of the distribution of devices or software that fail to adequately protect Keys and Certificates as required by the applicable Compliance Rules, and result in the unauthorized use or disclosure of such Keys and/or Certificates, Adopter shall be liable in an amount equal to its profits on such devices or software, but in no event less than \$1 million dollars nor more than \$8 million

10.3.3 Notwithstanding the foregoing, Adopter shall not be liable for liquidated damages if (a) Adopter maintains an internal program to assure compliance herewith (including a program to assure maintenance of inventory, samples, and confidentiality of information for purposes in addition to compliance with this Agreement), (b) the breach was inadvertent or otherwise unintentional, (c) the breach did not have a material adverse effect on the integrity or security of SmartRight Technology or the function of SmartRight Technology to protect Commercial Audiovisual Content and (d) if the Adopter was aware of the breach, it brought the breach to the Authority's attention in a timely manner

10.3.4 The parties agree and expressly acknowledge that amounts which may be payable by Adopter as contemplated in this Section 10.3 are a reasonable estimate of the damages that the Authority may sustain upon the occurrence of the events giving rise to such payments and that such amounts are reasonable and appropriate, since it would be impracticable or extremely difficult to determine the exact amount of the Authority's damages resulting from the specific acts giving rise to such payments. Said amounts are not to be construed in any sense to be a penalty and shall be considered adequate compensation to the Authority with respect to the acts giving rise to such payments.

10.4 Third Party Rights of Content Providers and Others. Compliance of Adopter and other licensees with the terms hereof is essential to maintain the value, integrity, security and performance of SmartRight Technology. As part of the consideration granted herein, upon Activation, Adopter agrees that (i) third parties who distribute or transmit, or cause or authorize the distribution or transmission of Marked Content, (ii) Content Participants (iii) and Fellow Adopters who are not in material breach of any term or condition of their Adopter Agreement are beneficiaries of this Agreement may bring a claim or action to enforce this Agreement against Adopter (a "Third Party Beneficiary Claim") in accordance with the procedures set out in the Procedural Rules. Such claims shall be limited to seeking injunctive relief against the manufacture, distribution, commercial use and sale of Adopter's products that are in material breach of the Compliance Rules, and against disclosure of Highly Confidential Information in breach of this Agreement that affects the integrity or security of SmartRight Technology, except

that where such Adopter has willfully breached, or engaged in a pattern or practice of breaching, such obligations, in which case attorneys' fees and costs shall be awarded to each third party that is a prevailing party.

Article XI. MISCELLANEOUS

11.1 **Ownership.** All SmartRight Technology provided by the Authority to Adopter shall remain the property of the Authority or its licensors. Except as expressly provided herein, this Agreement does not give Adopter any other license rights to the SmartRight Technology.

11.2 **Entire Agreement.** This Agreement, the exhibits hereto and the Specification constitute the entire Agreement between the parties hereto with respect to the subject matter hereof and supersede all prior oral, written or other agreements. Except as otherwise provided herein, this Agreement may not be modified except by written agreement dated subsequent to the date of this Agreement and signed by both parties.

11.3 **Controlled Entities.** Adopter represents and warrants that its Affiliates will comply with the terms of this Agreement and that it shall be responsible for the acts of its Affiliates to the same extent as if it performed those acts itself.

11.4 **Assignment.** The licenses granted hereunder are personal to Adopter, and Adopter's rights under this Agreement shall not be assigned or otherwise transferred except (a) with the written approval of the Authority (which shall not be unreasonably withheld) or (b) to a legal entity controlling, controlled by or under common control with Adopter or to the purchaser of all or substantially all of the outstanding capital stock or assets and obligations of Adopter or to the surviving entity in a merger, reorganization, or other business combination and where notice of such assignment has been provided in advance to the Authority and where the surviving or acquiring company agrees in writing to be bound by this Agreement. Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and permitted assigns. The Authority may assign or transfer this Agreement to a party that agrees to assume the Authority's obligations hereunder, and will provide Adopter with written notice thereof.

11.5 **Presumptions.** In construing the terms of this Agreement, no presumption shall operate in either party's favor as a result of its counsel's role in drafting the terms or provisions hereof.

11.6 Governing Law; Jurisdiction. THIS AGREEMENT, AND ALL THIRD-PARTY-BENEFICIARY CLAIMS BROUGHT PURSUANT HERETO, SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW YORK APPLICABLE TO AGREEMENTS MADE AND TO BE PERFORMED ENTIRELY IN SUCH STATE AND WITH THE LAWS OF THE UNITED STATES AS WOULD BE CONSTRUED BY A COURT SITTING IN THE SOUTHERN DISTRICT OF NEW YORK.

11.6.1 ANY LITIGATION BETWEEN THE PARTIES HERETO AND ANY THIRD-PARTY-BENEFICIARY CLAIM ARISING OUT OF OR RELATING TO THIS AGREEMENT SHALL BE SUBJECT (i) THE EXCLUSIVE JURISDICTION AND VENUE IN THE FEDERAL AND STATE COURTS LOCATED IN THE COUNTY OF NEW YORK, NEW YORK, (EXCEPT THAT CLAIMS BROUGHT PURSUANT TO SECTION 10.4 MAY BE BROUGHT IN A COURT SITTING IN LOS ANGELES COUNTY, CALIFORNIA); AND (ii) THE SERVICE OF PROCESS OF SAID COURTS BY PERSONAL DELIVERY OR BY MAILING OF PROCESS BY REGISTERED OR CERTIFIED MAIL, POSTAGE PREPAID, AT THE ADDRESSES SPECIFIED IN THIS AGREEMENT.

11.6.2 ADOPTER SHALL APPOINT AN AGENT IN THE STATE OF NEW YORK FOR ACCEPTANCE OF SERVICE OF PROCESS PROVIDED FOR UNDER THIS AGREEMENT AND SHALL NOTIFY THE AUTHORITY OF THE IDENTITY AND ADDRESS OF SUCH AGENT WITHIN THIRTY (30) DAYS AFTER THE EFFECTIVE DATE

11.6.3 ADOPTER WAIVES ANY OBJECTION TO THE JURISDICTION, PROCESS, AND VENUE OF ANY SUCH COURT, AND TO THE EFFECTIVENESS, EXECUTION, AND ENFORCEMENT OF ANY ORDER OR JUDGMENT (INCLUDING, BUT NOT LIMITED TO, A DEFAULT JUDGMENT) OF SUCH COURT PERTAINING TO THIS AGREEMENT, IN ANY OTHER JURISDICTION TO THE MAXIMUM EXTENT PERMITTED BY THE LAW OF THE PLACE WHERE ENFORCEMENT OR EXECUTION OF ANY SUCH ORDER OR JUDGMENT MAY BE SOUGHT AND BY THE LAW OF ANY PLACE WHOSE LAW MIGHT BE CLAIMED TO BE APPLICABLE REGARDING THE EFFECTIVENESS, ENFORCEMENT, OR EXECUTION OF SUCH ORDER OR JUDGMENT, INCLUDING PLACES OUTSIDE OF THE STATE OF NEW YORK AND OF THE UNITED STATES. ADOPTER AND THE AUTHORITY WAIVE ANY RIGHTS THEY MAY HAVE TO A JURY TRIAL.

11.7 Notice. All notices to be provided pursuant to this Agreement shall be given in writing and shall be effective when either served by personal delivery or upon receipt via certified mail, return receipt requested, postage prepaid, overnight courier service or sent by facsimile transmission with hard copy confirmation sent by certified mail, in each case to the party at the addresses set out herein.

11.8 Severability; Waiver. Should any part of this Agreement judicially be declared to be invalid, unenforceable, or void by any court of competent jurisdiction, the parties agree that the part or parts of this Agreement so held to be invalid, unenforceable, or void shall be reformed by such court without further action by the parties hereto but only to the extent necessary to make such part or parts valid and enforceable. A waiver by either of the parties hereto of any of the covenants to be performed by the other party or any breach thereof shall not be effective unless made in writing and signed by the waiving party and shall not be construed to be a waiver of any succeeding breach thereof or of any covenant herein contained.

11.9 Most Favored Status. The Authority will make available to Adopter the terms of its current standard Adopter Agreement, and any clarifications or interpretations of the provisions of its Adopter Agreement by posting them on the Authority website or otherwise. The Authority also commits that the benefit of any modification, clarifications or interpretations of language in the standard Adopter Agreement will be extended to Adopter in accordance with this section. Where the Authority agrees to make a change to a particular Fellow Adopter's standard Adopter Agreement, such change shall be reflected in the next regular revision of the standard Adopter Agreement. Upon the promulgation of such revision, Adopter will be given the option to substitute such revised Adopter Agreement for this Agreement. Prior to such time as it makes a revised standard Adopter Agreement available to all Fellow Adopters that have executed a standard Adopter Agreement, where the Authority has agreed to include language in a particular Fellow Adopter's standard Adopter Agreement that is more favorable than that in the then-current version of the standard Adopter Agreement, the Authority will not enforce the language in Adopter's Adopter Agreement to the extent that such language is less favorable than that found in such Fellow Adopter's Adopter Agreement. For purposes of this Section 11.9, "standard Adopter Agreement" refers to an Adopter Agreement under which a Fellow Adopter receives a license with respect to activities that are equivalent to all activities licensed hereunder, but does not include, by way of example and not limitation, any Adopter Agreement in which a Fellow Adopter is not licensed to manufacture or to sell Licensed Products.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first above written.

THE AUTHORITY:

ADOPTER:

By: _____

By: _____

Name:

Name:

Title:

Title:

Date:

Date:

Addresses for notices:

THE AUTHORITY:

ADOPTER:

SMARTRIGHT LICENSE AGREEMENT

EXHIBIT A

PROCEDURAL RULES EFFECTIVE JANUARY 1, 2004

Unless otherwise expressly stated in this Procedural Rules, all section references in this Procedural Rules are references to sections of this Procedural Rules.

1. FEE SCHEDULE

1.1 Annual, Certified Key and Per Unit Fees:

| Category of License | Annual Administration Fee | Certified Key Fee | Per Unit License Fee (SmartRight Label) |
|---------------------|---------------------------|-------------------|---|
| Evaluation Rights | \$10,000 | \$0.10 | N/A |
| Production Rights | \$30,000 | \$0.10 | \$2.00 |

Shipping and Handling: \$200 per order.

All Certified Keys are Highly Confidential Information and shall be subject to the requirements of section 7.3.1 of the Adopter Agreement.

1.2 **Procedure For Ordering Keys and SmartRight Labels.** Adopter will be supplied with a form and associated tools for ordering Keys and SmartRight Labels. The number of Keys and SmartRight Labels that may be ordered will be constrained to the Adopter's reasonably anticipated production run rate. There will be no refunds for unused Keys or SmartRight Labels.

2. REVOCATION AND RENEWAL PROCEDURES

2.1 **Request for Revocation.** Upon its own initiative, or at the request of a third party or parties whose rights have been adversely affected, the Association may re-

quest a Revocation of a Key or Keys by notifying the Registered Owner of the SmartRight Product containing the Key of the grounds upon which such Revocation is sought.

2.2 Revocation by Consent. In the event that Revocation is requested by the Registered Owner of one or more specified SmartRight Products, or such Registered Owner consents to a request by the Association, the Association shall Revoke the Keys which are the subject of the request without further proceedings. The cost of such Revocation shall be borne by the party making the request.

2.3 Procedure for Contested Revocation Within 30 days following issuance by the Association of a Request for Revocation, the owner of any SmartRight Product which is the subject of the Request may notify the Association of any objections to the request and the grounds therefore. Upon receipt of such objection, the Association shall take such measures as it deems appropriate to investigate and ascertain (a) whether grounds exist for Revocation and (b) whether such grounds constitute a sufficient threat to the integrity of the SmartRight System to justify the Revocation.

2.4 Judicial Review. The determination to Revoke or Renew a Key or Renew any SmartRight Products shall be made solely in the discretion of the Authority giving due regard to the interests of content owners, content distributors, adapters and device owners whose interests may be affected thereby, and shall be subject to review in accordance with the procedures set forth in Article 78 of the New York Civil Practice Law and Rules upon the grounds set forth in section 7803, subdivision 3 thereof.

2.5 Request for Renewal. Upon its own initiative or upon the request of any third party whose rights have been adversely affected, the Association may decide to implement Renewal of one or more SmartRight Products.

2.6 Implementation of Renewal. The Association shall delay the implementation of any Renewal for a sufficient period of time to ensure a smooth transition from the old system to the Renewed system. During that period, all Registered Owners of SmartRight Products affected by the Renewal shall either be sent new SmartRight Smart Cards free of charge, or provided with the opportunity to acquire such cards free of charge, at a location or locations established for that purpose, and any Certified Keys issued to Adopters who have not yet sold devices containing such keys, or to distributors or retailers of such devices who have not resold the devices to consumers, shall be replaced.

3. PROCEDURES FOR THIRD PARTY BENEFICIARY CLAIMS

3.1 Prior to initiating or instituting an action to enforce any Third Party Beneficiary Claim under section 10.4 of the Adopters Agreement, the party seeking to make such claim (the “Third Party Beneficiary”) shall provide the Authority notice and consultation reasonable under the circumstances regarding its proposed claim; provided that such consultation with the Authority shall not affect such party’s discretion to commence an action.

3.2 Promptly upon commencement of any action based on a Third Party Beneficiary Claim, the Third Party Beneficiary shall provide the Authority with notice of the commencement of any Action based on a Third Party Beneficiary Claim (a "Claim Notice") and, upon the Authority's request, copies of material documents supporting the claim.

3.3 Within 30 days following the receipt of a Claim Notice the Association and any Adopter may, at its option, join as an indispensable party to the action and Third-Party Beneficiary and the Defendant shall not object to, any motion to so join. Any judgment entered upon such claim relating to the interpretation or enforceability of any provision of this Agreement shall be binding on the Authority and any Adopters that failed to join such Beneficiary Claim as if they had joined such action.

3.4 The Authority shall cooperate reasonably with the parties to any Third Party Beneficiary Claim by providing appropriate and necessary information to the extent that such cooperation is consistent with the preservation of the integrity and security of SmartRight Technology and to the extent such cooperation does not involve release of Confidential Information to a party not subject to an agreement with the Authority to protect the confidentiality of such information.

3.5 Third Party Beneficiaries and Adopter shall not enter into any settlement that: (i) amends any material term of any Adopter Agreement or Associate Founder Agreement; (ii) has an adverse effect on the integrity, performance and/or security of SmartRight Technology or on the operation of SmartRight™ Technology with respect to protecting Commercial Audiovisual Content from any unauthorized output, transmission, interception or copying, or (iii) affects any of the rights of the Authority or its Licensors in and to SmartRight Technology or any intellectual property right embodied therein, unless the Authority shall have provided prior written consent thereto.

3.6 Nothing contained in these third party beneficiary procedures is intended to limit remedies or relief available pursuant to statutory or other claims that any party may have independent of its rights as a beneficiary of the Adopters Agreement.

SMARTRIGHT ADOPTERS AGREEMENT

EXHIBIT B

COMPLIANCE RULES EFFECTIVE JANUARY 1, 2004

INTRODUCTION

1. **DEFINITIONS.** The following definitions shall apply to this Exhibit B. Where a capitalized term is used but not otherwise defined in this Exhibit B, the meaning ascribed thereto elsewhere in the Agreement shall apply.

1.1 “Acquisition Device” means a SmartRight Product capable of receiving Conditional Access Content and/or Unencrypted Digital Terrestrial Broadcast Content.

1.2 “Add-in Device.” means a SmartRight Product, such as a Computer bus card, that passes content to another product other than where such product passes, or directs such content to be passed to an output (e.g. where a demodulator add-in card in a personal computer passes such content to an associated software application installed in the same computer).

1.3 “Authorized Digital Protection Technology” means SmartRight Technology or another technology approved by the United States Federal Communications Commission pursuant to 73 C.F.R §9008

1.4 “Broadcast Flag” means the Redistribution Control descriptor (rc_descriptor()) described in ATSC Standard A/65B: “Program and System Information Protocol for Terrestrial Broadcast and Cable.

1.5 “Combination Device” means a SmartRight Product which can perform the functions of an Acquisition Device and a Presentation Device.

1.6 “Commercial Audiovisual Content” shall mean audiovisual works, as defined in section 101 of the United States Copyright Act, which are (a) not created by the user of the Licensed Product and (b) offered for transmission, delivery or distribution, either generally or on demand, to subscribers or purchasers or the public at large, or otherwise for commercial purposes, not uniquely to an individual or a small, private group.

1.7 “Access Control System” means any commercially adopted technological method or system which effectively controls access to Commercial Audiovisual Content, such as SmartRight, DTCP, CSS, Digicypher, Harmony, DBS and other commercially-

adopted access control technology, including digitally-controlled analog scrambling systems, whether now or hereafter in commercial use.

1.8 “Computer Product” shall mean a product which is designed for or permits the end user to install a wide variety of commercially available software applications, including applications, such as a personal computer, handheld “Personal Digital Assistants,” and the like and further including subsystems of such a product, such as a graphics card.

1.9 “Conditional Access Content” means Commercial Audiovisual Content delivered to an Acquisition Device through a Conditional Access Delivery Method.

1.10 “Conditional Access Delivery Method” shall mean any medium or service which employs an Access Control System. Without limitation, “Conditional Access Delivery Methods” include Prerecorded Media, Pay Television Transmission; Pay-Per-View; Video-on-Demand; Subscription-on-Demand and Non-Premium Subscription Television, but shall not include content received through retransmission of a broadcast transmission (i.e., an over-the-air transmission for reception by the general public using radio frequencies allocated for that purpose) that, substantially simultaneously, is made by a terrestrial television broadcast station located within the country or territory in which the entity further transmitting such broadcast transmission also is located, where such broadcast transmission is not subject to a Commercially-Adopted Access Control Method (e.g., is broadcast in the clear and supported by advertising revenues or government mandated fees, without any other charge to members of the public receiving such broadcasts), regardless of whether such entity subjects such further transmission to an access control method. Notwithstanding the foregoing, Conditional Access Delivery Content shall include any service, Program, or schedule or group of Programs, that both (a) was primarily authored in a format with a resolution equal to or greater than 1000i or 700p (“High Definition”) and (b) is transmitted via a Commercially-Adopted Access Control Method in High Definition, provided that such service, Program, or schedule or group of Programs, is not, substantially simultaneously, transmitted in High Definition by a terrestrial broadcast station located within the same country or territory as Unencrypted Digital Terrestrial Broadcast Content..

1.11 “Consensus Watermark” shall mean a watermark technology designated as the “Consensus Watermark” by the Authority.

1.12 “Constrained Image” shall mean an image operating in a mode compatible with the Digital Visual Interface (DVI) Rev. 1.0 Specification as an image having the visual equivalent of no more than 350,000 pixels per frame (e.g., an image with resolution of 720 pixels by 480 pixels for a 4:3 aspect ratio), and 30 frames per second. A Constrained Image may be attained by reducing resolution, for example, by discarding, dithering, or averaging pixels to obtain the specified value. A Constrained Image can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image. By way of example, a Constrained Image may be stretched or doubled, and displayed full-screen, on a 1000-line monitor.

1.13 “Copy Freely” refers to Commercial Audiovisual Content which, as set out in the Specification, has been encoded by an Access Control System so that copy control is not asserted, but which remains subject to the rights of the copyright owner.

1.14 “Copy Once” refers to Commercial Audiovisual Content which, as set out in the Specification, has been encoded by an Access Control System as “Copy Once” indicating that only one generation of copies may be made of it following decryption.

1.15 “Copy Never” refers to Commercial Audiovisual Content which, as set in the Specification, has been encoded by an Access Control System so that no copying is permitted following decryption.

1.16 “Copyright Watermark” shall mean the watermark technology designated in the Specification as the “Copyright Watermark.”

1.17 “Covered Demodulator Product” means an Acquisition Device or other product that is required under 47 CFR §§ 73.9002(a)(1) or 73.9002(b)(1) to comply with the Demodulator Compliance Requirements, and to be manufactured in accordance with the Demodulator Robustness Requirements of 73 CFR 9007.

1.18 “Decrypted SmartRight Content” means SmartRight Content that has been decrypted by a Presentation Device.

1.19 “Designated Watermarks” means the Copyright Watermark and, 18 months following its designation by the Authority, the Consensus Watermark.

1.20 “Digital Rights Management Method” means a technological measure that effectively controls access to a copyrighted work.

1.21 “Encrypted SmartRight Content” means SmartRight Content that has not been decrypted by a Presentation Device.

1.22 “EIT” means the Event Information Table as defined in ATSC Standard A/65B: “Program and System Information Protocol for Terrestrial Broadcast and Cable.”

1.23 “EPN Field” shall mean the field or bits, described in the Specification, used to indicate that Commercial Audiovisual Content is to be protected using SmartRight, the SmartRight Usage State to be applied to such content and, optionally, an Out-bound Usage State.

1.24 “High Definition Analog Form” shall mean a format that is an analog video signal which has a resolution greater than a Constrained Image.

1.25 “High Definition Analog Output” shall mean an output capable of transmitting Commercial Audiovisual Content in High Definition Analog Form.

1.26 “Image Constraint Token” shall mean the field or bits, as described in the Specification, used to trigger the output of a “Constrained Image” in Access Control Systems.

1.27 “Marked Content” means (a) Unencrypted Digital Terrestrial Broadcast Content for which an Acquisition Device has received, demodulated and either the EIT or the PMT inspected and determined the Broadcast Flag to be present or (b) Unencrypted SmartRight Content which was previously determined by an Acquisition Device to have been Marked Content.

1.28 “Non-Premium Subscription Television” shall mean a Conditional Access Delivery of a service, or schedule or group of Programs (which may be offered for sale together with other services, or schedule or group of Programs), for which subscribers are charged a subscription fee for the reception or viewing of the programming contained therein, other than Pay Television Transmission and Subscription-on-Demand. By way of example, “basic cable service” and “extended basic cable service” in the United States (other than such programming contained therein that does not fall within the definition of Conditional Access Delivery) are “Non-Premium Subscription Television.”

1.29 “Outbound Usage State” is the usage state that is applied by a Presentation Device to determine the output rules applicable to the exportation of Decrypted SmartRight Content to other Control Access Systems. The permitted Output Usage States are Copy Freely, Copy Once, Copy Never and Output Forbidden.

1.30 “Output Forbidden” refers to the Outbound Usage State which specifies that Decrypted SmartRight Content may not be passed to any output.

1.31 “Pay-Per-View” shall mean a delivery of a single Program or a specified group of Programs, as to which each such single Program is generally uninterrupted by Commercial Advertising Messages and for which recipients are charged a separate fee for each Program or specified group of Programs. The term “Pay-Per-View” shall also include delivery of a single Program as described above for which multiple start times are made available at time intervals which are less than the running time of such Program as a whole. If a given delivery qualifies both as Pay-Per-View and a Pay Television Transmission, then, for purposes of this Agreement, such delivery shall be deemed Pay-Per-View rather than a Pay Television Transmission.

1.32 “Pay Television Transmission” shall mean a transmission of a service or schedule of Programs, as to which each individual Program is generally uninterrupted by Commercial Advertising Messages and for which service or schedule of Programs subscribing viewers are charged a periodic subscription fee, such as on a monthly basis, for the reception of such programming delivered by such service whether separately or together with other services or programming, during the specified viewing period covered by such fee. If a given delivery qualifies both as a Pay Television Transmission and Pay-Per-View, Video-on-Demand, or Subscription-on-Demand then, for purposes of this Agreement, such delivery shall be deemed Pay-Per-View, Video-on-Demand or Subscription-on-Demand rather than a Pay Television Transmission.

1.33 “Peripheral TSP Product” means a product that is capable of accessing in usable form Unscreened Content or Marked Content passed to such product via a Robust Method where the manufacturer of such product has committed in writing in accordance with § 73.9002(c) that such product will comply with the Demodulator Compliance Requirements and be manufactured in accordance with the Demodulator Robustness Requirements.

1.34 “Output Categories” mean the categories of video output for which Outbound Usage States may be specified for Decrypted SmartRight Content exported to another Access Control System. The Output Categories which may be specified for Decrypted SmartRight Content include (a) standard definition analog output, (b) high definition analog output, (c) uncompressed digital output and (d) compressed digital output.

1.35 “PMT” means Program Map Table as defined in International Standard ISO/IEC 13818-1:2000(E): “Information Technology – Generic Coding of Moving Pictures and Associated Audio Information: Systems”

1.36 “Prerecorded Media” shall mean the delivery of one or more Programs, in prerecorded and encrypted or scrambled form, on packaged media, such as DVD discs.

1.37 “Presentation Device” means a SmartRight Product capable of decrypting Encrypted SmartRight Content.

1.38 “Private Copy” refers to the SmartRight Usage State specifying that such content may be freely copied, but may only be displayed by Presentation Devices within a particular Personal Private Network.

1.39 “Program” shall mean any work of Commercial Audiovisual Content.

1.40 “Retention State Field” shall mean the field or bits, as described in the Specification, used to specify the time period during which a Session Key can be decrypted by a Presentation Device.

1.41 “Robust Method” means a data path which complies with Section 2 of the Compliance Rules.

1.42 “Session Key” means a Key generated by a Converter Card for decrypting the LECM of View Only SmartRight Content. A Session Key is stored solely in the converter card which converted the content during the period designated in the Retention State Field.

1.43 “SmartRight Usage State” means the usage state that is specified in the LECM for encrypted SmartRight Content. The permitted SmartRight Usage states are Copy Freely, Private Copy and View Only.

1.44 “Standard Definition Analog Output” means an NTSC, YUV, SECAM, PAL, or consumer RGB format analog output (including an S-video output for the listed

formats) that carries uncompressed video signals with a resolution less than or equal to a Constrained Image.

1.45 “Storage Only Device” means a SmartRight Product which can store or record Encrypted SmartRight content, but which does not perform the functions of an Acquisition Device or a Presentation Device.

1.46 “Subscription-on-Demand” shall mean the delivery of a single Program or a specified group of Programs for which (i) a subscriber is able, at his or her discretion, to select the time for commencement of exhibition thereof; (ii) where each such single Program is generally uninterrupted by Commercial Advertising Messages; and (iii) for which Program or specified group of Programs subscribing viewers are charged a periodic subscription fee for the reception of programming delivered by such service during the specified viewing period covered by the fee. In the event a given delivery of a Program qualifies both as a Pay Television Transmission and Subscription-on-Demand, then for purposes of this Agreement, such delivery shall be deemed Subscription-on-Demand rather than a Pay Television Transmission.

1.47 “Transitory Image” shall mean data which has been stored temporarily for the sole purpose of enabling the immediate display of content but which (a) does not persist materially after the content has been displayed and (b) is not stored in a way which permits copying or storing of such data for other purposes.

1.48 “Unencrypted Digital Terrestrial Broadcast Content” means Commercial Audiovisual Content contained in the signal broadcast by a digital television station without encrypting or otherwise making the content available through a technical means of conditional access, and includes such content when retransmitted in unencrypted digital form.

1.49 “Unscreened Content” means, with respect to an Acquisition Device, Unencrypted Digital Terrestrial Broadcast Content that such product either (1) received and demodulated and for which such product has inspected neither the EIT nor the PMT for the Broadcast Flag or (2) has received via a Robust Method and accessed in usable form, and for which such product has inspected neither the EIT nor the PMT for the Broadcast Flag and has not determined through information robustly conveyed with such content another Covered Demodulator Product had previously so screened such content and determined the Broadcast Flag to be present; provided, however, that, with respect to a Covered Demodulator Product, “Unscreened Content” shall not include content that has been passed from such product pursuant to Section 2.1 of these rules.

1.50 “User Accessible Bus” means a data bus that is designed for end user upgrades or access, such as an implementation of a smartcard interface, PCMCIA, Cardbus, or PCI that has standard sockets or otherwise readily facilitates end user access. A “User Accessible Bus” does not include memory buses, CPU buses, or similar portions of a device's internal architecture that do not permit access to content in a form usable by end users.

1.51 “Video-on-Demand” shall mean a delivery of a single Program or a specified group of Programs for which (i) each such individual Program is generally uninterrupted by Commercial Advertising Messages; (ii) recipients are charged a separate fee for each such single Program or specified group of Programs; and (iii) a recipient is able, at his or her discretion, to select the time for commencement of exhibition of such individual Program or specified group of Programs. In the event a delivery qualifies as both Video-on-Demand and a Pay Television Transmission, then for purposes of this Agreement, such delivery shall be deemed Video-on-Demand.

1.52 “View Only” refers to Commercial Audiovisual Content which, as set out in the Specification, has been encoded as “View Only,”

2. COMPLIANCE RULES APPLICABLE TO UNENCRYPTED DIGITAL TERRESTRIAL BROADCAST CONTENT.

2.1 Unscreened Content.

(a) **Output of Unscreened Content.** A SmartRight Product shall not pass, or direct to be passed, Unscreened Content to any output except:

- (i) to an analog output;
- (ii) to an 8-VSB, 16-VSB, 64-QAM or 256-QAM modulated output, provided that the Broadcast Flag is retained in the both the EIT and PMT;
- (iii) to a digital output protected by an Authorized Digital Output Protection Technology authorized for use with Unscreened Content, in accordance with any applicable obligations established as a part of its approval pursuant to 47 CFR §73.9008;
- (iv) where the stream containing such content has not been altered following demodulation and such Covered Demodulator Product outputs, or directs to be output, such content to a Peripheral TSP Product solely within the home or other, similar local environment, using a Robust Method;
- (v) where such product outputs, or directs to be output, such content for the purpose of making a recording of such content pursuant to paragraph (b)(ii) of this section, where such content is protected by the corresponding recording method; or
- (vi) where such Covered Demodulator Product is incorporated into a Computer Product and passes, or directs to be passed, such content to an unprotected output operating in a mode compatible with the Digital Visual Interface (DVI) Rev. 1.0 Specification as an image having the visual equivalent of no more than 350,000 pixels per frame (e.g. an image with resolution of 720 x 480 pixels for a 4:3 (nonsquare pixel) aspect ratio), and 30 frames per second. Such an image may be attained by reduc-

ing resolution, such as by discarding, dithering or averaging pixels to obtain the specified value, and can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

(b) **Recording of Unscreened Content.** SmartRight Products shall not record or cause the recording of Unscreened Content except by:

(i) a method that effectively and uniquely associates such recording with a single Device (using cryptographic protocol or other effective means) so that such recording cannot be accessed in usable form by another product except where the content of such recording is passed to another product as permitted under these Rules or

(ii) an Authorized Recording Method approved by the United States Federal Communications Commission for use with Unscreened Content pursuant to 47 C.F.R. § 73.9008 (provided that for recordings made on removable media, only Authorized Recording Methods expressly approved pursuant to 47 C.F.R. § 73.9008 for use in connection with removable media may be used).

(c) Paragraph (b) of this section does not impose restrictions regarding the storage of Unscreened Content as a Transitory Image.

2.2 **Marked Content:**

(a) **Output of Marked Content.** A SmartRight Product shall not pass, or direct to be passed, Marked Content to any output except

(i) to an analog output;

(ii) to an 8-VSB, 16-VSB, 64-QAM or 256-QAM modulated output, provided that the Broadcast Flag is retained in the both the EIT and PMT;

(iii) to a digital output protected by an Authorized Digital Output Protection Technology, in accordance with any applicable obligations established as a part of its approval pursuant to 47 C.F.R. § 73.9008;

(iv) as Private Copy Encrypted SmartRight Content.

(v) where such product outputs, or directs to be output, such content for the purpose of making a recording of such content pursuant to paragraph (b)(2) of this section; where such content is protected by the corresponding recording method; or

(vi) where such Product is incorporated into a Computer Product and passes, or directs to be passed, such content to an unprotected output operating in a mode compatible with the Digital Visual Interface (DVI) Rev. 1.0 Specification as an image having the visual equivalent of no more than 350,000 pixels per frame (e.g., an image with resolution of 720 x 480 pixels for a 4:3 (nonsquare pixel) aspect ratio), and 30

frames per second. Such an image may be attained by reducing resolution, such as by discarding, dithering or averaging pixels to obtain the specified value, and can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

(b) A SmartRight Product shall not record or cause the recording of Marked Content in digital form unless such recording is made using one of the following methods:

(i) as Encrypted SmartRight Content, or using another method that effectively and uniquely associates such recording with a single Covered Demodulator Product (using a cryptographic protocol or other effective means) so that such recording cannot be accessed in usable form by another product except where the content of such recording is passed to another product as permitted under this subpart or

(ii) an Authorized Recording Method in accordance with any applicable obligations established as a part of its approval by the FCC pursuant to 47 C.F.R. §73.9008 (provided that for recordings made on removable media, only Authorized Recording Methods expressly approved by the FCC pursuant to 47 C.F.R. §73.9008 for use in connection with removable media may be used).

(c) Paragraph (b) of this section does not impose restrictions regarding the storage of Marked Content as a Transitory Image.

2.3 Output Restrictions on Audio. Except as otherwise provided in §§2.1(a) or 2.2(a), Covered Demodulator Products shall not output the audio portions of Unscreened Content or of Marked Content in digital form except in compressed audio format (such as AC3) or in Linear PCM format in which the transmitted information is sampled at no more than 48 kHz and no more than 16 bits/sample.

2.4 Add-In Devices. Where an Add-In Device passes Unscreened Content or Marked Content to another product, other than where such Covered Demodulator Product passes, or directs such content to be passed to an output (e.g., where a demodulator add-in card in a personal computer passes such content to an associated software application installed in the same computer), it shall pass such content:

(a) using a Robust Method; or

(b) as Encrypted SmartRight Content or using Authorized Digital Output Protection Technology authorized for such content in accordance with any applicable obligations established as a part of its approval by the FCC pursuant to 47 C.F.R. §73.9008. Neither Unscreened Content nor Marked Content may be so passed in unencrypted, compressed form via a User Accessible Bus.

2.5 Unmarked Content. SmartRight Products shall place no restrictions on the output, recording or display of Unencrypted Terrestrial Broadcast Content which is not Unscreened Content or Marked Content.

3. COMPLIANCE RULES APPLICABLE TO ACQUISITION DEVICES.

3.1 **Communications Capability.** All Acquisition Devices shall have a digital communications port communicate over a digital network with other SmartRight Products using a protocol in accordance with the Specification

3.2 **Inspection of Unencrypted Digital Terrestrial Broadcast Content for Broadcast Flag.** All Acquisition devices which (a) receive and demodulate Unencrypted Digital Terrestrial Broadcast Content, or have received such content in usable form via a Robust Method from a Covered Demodulator Product shall inspect either the EIT or the PMT of all Unencrypted Digital Terrestrial Broadcast Content prior to any digital output to determine the presence of the Broadcast Flag. In the event such inspection determines that the Broadcast Flag is present, the Marked Content shall be converted by the Acquisition Device into Private Copy Encrypted SmartRight Content.

3.3 **Inspection of Conditional Access Content.**

(a) All Acquisition Devices which receive Conditional Access Content shall inspect such content prior to output to determine the presence of an EPN Field and the contents thereof.

(b) Following the implementation of the Consensus Watermark, as provided in section 8.2(i), all acquisition devices which receive unencrypted Conditional Access Content shall inspect such content prior to any output to determine the existence of a Consensus Watermark.

3.4 **Conversion of SmartRight Content.**

(a) Marked Content and unencrypted Conditional Access Content containing an EPN field or a Consensus Watermark will be encrypted by the Acquisition Device. The encryption will preserve the Broadcast Flag, the Designated Watermarks, and any information included in the content for use by other Access Control Methods.

(b) The Converter Card will generate an LECM to be packaged with the Encrypted Content by the Acquisition Device in accordance with the Specification which shall contain the information required by authorized Presentation Devices to decrypt the content and enforce the Usage States associated therewith, including whether the content was Marked Content and the appropriate SmartRight Usage State and any Output Usage State designated by the EPN Field.

(c) The LECM for Copy Freely SmartRight Content shall not be encrypted.

(d) The LECM for Private Copy and View Only SmartRight Content shall be encrypted by a Converter Card connected to the PPN using the Network Key applicable to the PPN with which the Device is associated, as defined by Specifications.

(e) In addition, The LECM for View Only SmartRight Content shall be super-encrypted using a Session Key generated by a Converter Card which is not stored with the SmartRight Content but is retained in the Converter Card only for the period of time designated in the Retention State Field.

3.5 **Output Restrictions.**

(a) **SmartRight Content.** SmartRight Content may not be output by any Acquisition Device except to a digital output in the form of Encrypted SmartRight Content.

(b) **Compatibility with Other Systems.** Nothing in the Specification or these Compliance Rules shall interfere with or prevent any Acquisition Device from complying with any restrictions on the output Controlled Access Content imposed by any other Access Control Method.

(c) **Consensus Watermark.** Acquisition Devices will comply with the rules applicable to unscrambled content containing the Consensus Watermark as provided in Section 8.2 below.

3.6 **Storage and Recording Restrictions.**

(a) **SmartRight Content.** An Acquisition Device shall not record or cause the recording of SmartRight Content except Encrypted SmartRight Content may be recorded in digital form such that only an authorized Presentation Device can decrypt the content.

(b) **Non-SmartRight Controlled Access Content.** Nothing in the Specification or these Compliance Rules shall interfere with or prevent any Acquisition Device from complying with any restrictions on storage or recording of Controlled Access Content imposed by any other Access Control Method.

(c) The restrictions imposed by this section do not apply to internal storage of content as a Transitory Image.

4. **COMPLIANCE RULES APPLICABLE TO PRESENTATION DEVICES**

4.1 **Communications Capability.** All Presentation Devices shall have a digital communications port which permits it to communicate over a digital network with other SmartRight Products in accordance with the Specification.

4.2 **Key Generation.**

(a) **Network Keys.**

(i) Upon connection to a PPN, a Presentation Device will communicate with any other Presentation Device, as provided in the Specification, to determine whether a Network Key has been generated.

(ii) If no other Presentation device is connected to the PPN, the Terminal Module will generate and store a new Network Key.

(iii) If other Presentation Devices are connected to the PPN and the Maximum Network Size has not previously been reached, the Terminal Module will store the existing Network Key.

(iv) No more than one Network Key may be stored in any Terminal Module. Once a Network Key has been stored in a Terminal Module, it will not store a new Network Key until the previous Key has been erased.

4.3 **Decryption of SmartRight Content.**

(a) **Copy Freely.** All Presentation Devices may decrypt Copy Freely Encrypted SmartRight Content

(b) **Private Copy.** All Private Copy SmartRight Content shall be decrypted using the Network Key applicable to the PPN with which the Presentation Device is associated. Any View Only or Private Copy SmartRight Content packaged with a different Network Key shall not be processed.

(c) **View Only.** View Only SmartRight Content shall be decrypted using a Session Key stored in an Acquisition Device which encrypted the content within the time period specified in the Retention State Field. Any View Only SmartRight Content for which a Session Key is not stored in an Acquisition Device connected to the PPN shall not be processed.

(d) **Preservation of Control Information.** The decryption of SmartRight Content by a Presentation Device shall preserve the Broadcast Flag and any information included in the content for use by other Access Control Methods.

4.4 **Compatibility with other Protection Systems**

(a) Nothing in the Specification or these Rules shall prohibit or interfere with the ability of a Presentation Device to receive or process information in compliance with any other Access Control Method.

(b) All Presentation Devices capable of displaying a video image with resolution greater than a Constrained Image shall respond to the Constrained Image Token.

4.5 **Output Control of Decrypted SmartRight Content**

(a) **Marked Content.** Marked Content which has been decrypted by a Presentation Device may not be passed to any output except as authorized by section 2.2.

(b) **Conditional Access Content.** A Presentation Device shall not pass the Decrypted SmartRight Content other than Marked Content to any output except as follows:

(i) Presentation Devices that are not configured to export content to other Access Control Systems by a Robust Method may only output Decrypted SmartRight Content with a Copy Freely Outbound Usage State applicable to such Output Category. For example, Decrypted SmartRight Content with an Outbound User State of Copy Freely for Standard Definition Analog Output but as Copy Never for all other Outputs may only be passed to a Standard Definition Analog Output.

(ii) A Presentation Device configured to export Decrypted SmartRight content to another Access Control System shall assign an Outbound Usage State corresponding to the SmartRight Usage State to any Decrypted SmartRight content that was not assigned an Outbound Usage State by the EPN Field, as follows:

| SmartRight Usage State | Outbound Usage State |
|------------------------|----------------------|
| Copy Freely | Copy Freely |
| Private Copy | Copy Never |
| View Only | Copy Never |

(iii) Presentation Devices configured to export content to other Access Control Systems may direct output to any Output Category which provides a level of protection sufficient to provide the at least same degree of protection specified by the Outbound Usage State for that Output Category. If the Access Control System does not provide the same level of protection designated by the Outbound Usage State, but provides a higher level of protection, the content may be exported to that system with a Usage State requiring that higher level of protection. For example, content designated as Copy Never for uncompressed digital output and Copy Once for all other Output Categories may be output to a DVI or DTCP device but may not be output to a system that does not provide any protection for analog output. Such content may also be designated as Copy Never and output to an Access Control System that does not provide Copy Once protection to all Output Categories, but provides Copy Never protection.

4.6 **Recording and Storage of Decrypted Smart Right Content.** Decrypted SmartRight Content may not be recorded or stored by a Presentation Device except as follows:

4.7 **Marked Content** Recording and Storage of Marked Content shall be governed by section 2.2(b)

4.8 **Conditional Access Content;**

Any storage of decrypted View Only SmartRight Content shall be for a period no greater than the time the set out in the Retention State Field and shall be removed from storage following the expiration of that time.

(a) Decrypted Conditional Access Content other than View Only Content may be recorded pursuant to a recording method which permits no greater usage than would be allowed by an output authorized by section 4.5. For example, Decrypted SmartRight Content with a Copy Once Outbound Usage State for any or all outputs may be recorded in a manner which permits reproduction solely as Copy Never content, or the equivalent, by an Access Control System capable of enforcing that restriction.

5. COMPLIANCE RULES APPLICABLE TO COMBINATION DEVICES.

Combination Devices shall comply with all Compliance Rules set forth in articles 2, 3, 4, 7 and 8 of these Rules other than sections 3.5(a) and 3.6(a).

6. COMPLIANCE RULES APPLICABLE TO STORAGE ONLY DEVICES.

Storage Only Devices shall comply with all Compliance Rules set forth in articles 2, 3, 7 and 8 of these Rules other than sections 3.1, 3.2, 3.3, and 3.4.

7. PROTECTION AGAINST INTERNET TRANSMISSION AND “BOOT-LEG” COPIES.

7.1 All SmartRight Products shall apply the proximity control provisions of the Specification to determine whether SmartRight Content received through a digital communications port was transmitted through the public internet. SmartRight content which is determined to have been transmitted over the public internet without authorization shall not be decrypted, stored, recorded, displayed or output by the Device.

7.2 All SmartRight Products shall inspect any digital audiovisual content other than Encrypted SmartRight Content received in any manner other than by a Conditional Access Delivery Method or as Unencrypted Digital Terrestrial Broadcast Content for the presence of an EPN Field and the Broadcast Flag. Any such content containing the broadcast flag, or designated other than as Copy Freely by the EPN Field, shall not be decrypted, stored, recorded, displayed or output by the Device.

7.3 Following the implementation of the Consensus Watermark, as provided in section 8.2(i), all SmartRight Products shall inspect any digital audiovisual content other than Encrypted SmartRight Content received in any manner other than by a Conditional Access Delivery Method or as Unencrypted Digital Terrestrial Broadcast Content for the presence of the Consensus Watermark. Any such content designated Copy Never, or the equivalent, shall not be stored, recorded by the Device

8. **CONSENSUS AND COPYRIGHT WATERMARK IMPLEMENTATION**

8.1 **Pre-Implementation Protection of the Consensus Watermark.** Commencing on the date that the Authority identifies the Consensus Watermark and the Copyright Watermark, Adopter:

(i) Shall, when selecting among technological implementations for product features of Licensed Products designed after such date, take commercially reasonable care (taking into consideration the reasonableness of the costs of implementation, as well as the comparability of their technical characteristics, of applicable commercial terms and conditions, and of their impact on Decrypted Data and on the effectiveness and visibility of the Consensus Watermark) that SmartRight Products and components thereof do not strip, interfere with or obscure the Consensus Watermark.

(ii) Shall not design new products or components thereof for which the primary purpose is to strip, interfere with or obscure the Consensus Watermark; and

(iii) Shall not knowingly promote or knowingly advertise or knowingly cooperate in the promotion or advertising of products or components thereof for the purpose of stripping, interfering with or obscuring the Consensus Watermark.

8.2 **Protection of Designated Watermarks.** The following provisions are applicable to the Copyright Watermark and, with respect to all SmartRight Products manufactured within 18 months following its designation, to the Consensus Watermark.

(i) Acquisition Devices shall be designed to inspect unencrypted Conditional Access Content for the presence of a Consensus Watermark and shall convert such content to Encrypted Smart Right Content with the appropriate SmartRight Usage State and Outbound Usage State.

(ii) Presentation Devices shall not process any content containing a Copyright Watermark unless such content is received in the form of Encrypted SmartRight Content.

(iii) Adopter shall not produce Licensed Products or components thereof for which the primary purpose is to strip, interfere with or obscure a Designated Watermarks; and

(iv) Adopter shall not knowingly distribute or knowingly cooperate in distribution of Licensed Products or components thereof for the purpose of stripping, interfering with or obscuring the Designated Watermarks.

(b) **Product Features.** This Article 8 shall not prohibit a Licensed Product or Licensed Component from incorporating legitimate features (i.e., zooming, scaling, cropping, picture-in-picture, compression, recompression, image overlays, overlap of windows in a graphical user interface, audio mixing and equalization, video mixing and keying, downsampling, upsampling, and line doubling, or conversion between

widely-used formats for the transport, processing and display of audiovisual signals or data, such as between analog and digital formats and between PAL and NTSC or RGB and YUV formats, as well as other features as may be added to the foregoing list from time to time by the Authority by amendment to these Compliance Rules) that are not prohibited by law, and such features shall not be deemed to strip, interfere with or obscure the Designated Watermark, provided that (a) Adopter shall take commercially reasonable care that such features in a Licensed Product do not strip, obscure, or interfere with a Designated Watermark in Conditional Access Delivery Content received by such Licensed Product, and (b) Adopter shall not knowingly market or knowingly distribute, or knowingly cooperate in marketing or distributing, such Licensed Products or Licensed Components for the purpose of stripping, obscuring or interfering with a Designated Watermark in Conditional Access Delivery Content.

(c) Adopter is alerted that the requirements of this Article 8, and the declaration of the Consensus Watermark, may be rescinded by the Association if, during the two (2)-year period immediately preceding the fourth anniversary of such declaration, the Consensus Watermark has not been implemented by major content providers in more than thirty-three percent (33%) of DVD discs of new theatrical motion pictures produced for DVD released by such providers in the United States of America and Canada during such period.

EXHIBIT “C” ROBUSTNESS RULES

1. CONSTRUCTION

1.1 **Generally.** SmartRight Products as shipped shall meet the applicable Compliance Rules set forth in Exhibit B, and shall be manufactured in a manner so that they cannot be defeated or circumvented merely by an ordinary user using generally-available tools or equipment. Generally-available tools or equipment means tools or equipment that are widely available at a reasonable price, including but not limited to, screwdrivers, jumpers, clips and soldering irons. Generally-available tools or equipment also means specialized electronic tools or software tools that are widely available at a reasonable price, other than devices or technologies that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies used to meet the requirements set forth in this subpart. Such specialized electronic tools or software tools includes, but is not limited to, EEPROM readers and writers, debuggers or decompilers.

1.2 **Defeating Functions.** Licensed Products shall not include:

(a) switches, buttons, jumpers or software equivalents thereof,

(b) specific traces that can be cut, or

(c) functions (including service menus and remote-control functions),

in each case by which the mandatory provisions of the Specification or the Compliance Rules, including the content protection technologies, analog protection systems, output protections, output restrictions, recording protections or recording limitations can be defeated, or by which Unscreened Content, Marked Content or Conditional Access Content (collectively “Protected Content”) in such Licensed Products can be exposed to output, interception, retransmission or copying, in each case other than as permitted under this Agreement.

1.3 **Keep Secrets.** Licensed Products shall be manufactured in a manner that is clearly designed to effectively frustrate attempts to discover or reveal Keys and any other Highly Confidential Information.

1.4 **Robustness Checklist.** Before releasing any Licensed Product, Adopter must perform tests and analyses to assure compliance with these Robustness Rules. A Robustness Checklist is attached as Exhibit C-1 for the purpose of assisting Adopter in performing tests covering certain important aspects of these Robustness Rules. Inasmuch as the Robustness Checklist does not address all elements required for the manufacture of a Compliant product, Adopter is strongly advised to review carefully the Specification, Compliance Rules (including, for avoidance of doubt, these Robustness Rules) so as to

evaluate thoroughly both its testing procedures and the compliance of its Licensed Products. Adopter shall provide copies of the Specification, the Compliance Rules (including, for avoidance of doubt, these Robustness Rules) and the Robustness Checklist to its supervisors responsible for design and manufacture of Licensed Products.

2. DATA PATHS.

2.1 Unencrypted Content shall not be available on outputs other than those specified in the Compliance Rules

2.2 Protected Content decrypted by an Add in Device shall not be present on a User Accessible Bus in analog or unencrypted, compressed form.

2.3 Protected Content with an Outbound Usage State restricting its output to exportation to another device employing an Access Control System must be encrypted, compressed, encoded or otherwise output in accordance with the compliance rules of the destination Access Control System applicable to data moving from one device to another.

2.4 Adopter is alerted that these Robustness Rules may be revised in the future, upon notification by the Authority, to require that, when the Authority deems that it is technically feasible and commercially reasonable to do so, Licensed Products be designed such that content in a form in which is not permitted to be output under the compliance rules is not transmitted over a User Accessible Bus, is made reasonably secure from unauthorized interception by use of means that can be defeated by an ordinary user using generally available tools.

3. METHODS OF MAKING FUNCTIONS ROBUST. Licensed Products shall be manufactured using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the content protection requirements set forth below.

3.1 **Distributed Functions.,** Where Protected Content is delivered from one part of the Licensed Product to another, whether among integrated circuits, software modules, or otherwise or a combination thereof, the portions of the Licensed Product that perform authentication and decryption and the MPEG (or similar) decoder shall be designed and manufactured in a manner associated and otherwise integrated with each other such that data flowing in any usable form flowing between these portions of the Licensed Product shall be reasonably secure from being intercepted or copied except as authorized by the Compliance Rules.

3.2 **Software.** Any portion of the Licensed Product that implements any of the content protection requirements of the Specification or the Compliance Rules by Software shall comply with all of the requirements forth in Sections 1 and 2 of this Exhibit C. For the purposes of these Robustness Rules, "Software" shall mean the implementation of the content protection requirements as to which this Agreement requires a Licensed Product to be compliant through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware. Such implementations shall:

(a) Comply with Section 1.3 of this Exhibit C by a reasonable method including but not limited to: encryption, execution of a portion of the implementation in ring zero or supervisor mode, and/or embodiment in a secure physical implementation; and, in addition, in every case of implementation in Software, using techniques of obfuscation clearly designed to effectively disguise and hamper attempts to discover the approaches used.

(b) Be designed so as to perform self-checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide the authorized authentication and/or decryption function. For the purpose of this provision, a “modification” includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Sections 1 and 2 of this Exhibit C. This provision requires at a minimum the use of “signed code” or more robust means of “tagging” operating throughout the code.

3.3 Hardware. Any portion of the Licensed Product that implements any of the content protection requirements of the Specification or the Compliance Rules by Hardware shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit C. For the purposes of these Robustness Rules, “Hardware” shall mean a physical device other than a SmartRight Smart Card, including a Licensed Component that implements any of the content protection requirements as to which this Agreement requires that a Licensed Product be compliant and that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component; or (ii) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Licensed Product or Licensed Component and such instructions or (iii) data are not accessible to the end user through the Licensed Product or Licensed Component. Such implementations shall:

(a) Comply with Section 1.3 of this Exhibit C by any reasonable method including but not limited to embedding Device Keys and Highly Confidential cryptographic algorithms in silicon circuitry or firmware that cannot reasonably be read, or employing the techniques described above for Software.

(b) Be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the content protection requirements of SmartRight (including compliance with the Compliance Rules and Specification) in Licensed Products would pose a serious risk of rendering the Licensed Product unable to receive, decrypt, or decode SmartRight Content. By way of example, a component that is soldered rather than socketed may be appropriate for this means.

3.4 SmartRight Smart Cards. SmartRight Smart Cards shall include all of the characteristics set forth in Sections 1 and W of this Exhibit C. In particular, and without limiting the generality of the foregoing, all Terminal Cards shall comply with an ISO/IEC 15408 terminal card protection profile set of criteria applicable to all SmartRight Smart Cards as defined in the Specification.

3.5 **Hybrid.** The interfaces between Hardware and Software portions of a Licensed Product shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection which would be provided by a pure Software implementation.

3.6 **Level of Protection.** "Core Functions" of SmartRight include encryption, decryption, authentication, the limitations on use, storage, recording and output set forth in the Compliance Rules, maintaining the confidentiality of Highly Confidential cryptographic algorithms and Keys and preventing unauthorized exposure of Protected Content. The Core Functions of SmartRight shall be implemented in a reasonable method so that they cannot be defeated or circumvented merely by an ordinary user using generally-available tools or equipment.

3.7 **Advance of Technology.** Although an implementation of a Licensed Product when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of a particular Licensed Product, would have caused such products to fail to comply with these Robustness Rules ("New Circumstances"). If an Adopter has (a) actual notice of New Circumstances, or (b) actual knowledge of New Circumstances (the occurrence of (a) or (b) hereinafter referred to as "Notice"), then within eighteen (18) months after Notice such Adopter shall cease distribution of such Licensed Product and shall only distribute Licensed Products that are compliant with the Robustness Rules in view of the then-current circumstances.

4. EXAMINATION

4.1 **Generally.** If the Association so requests via the Authority, , Adopter shall provide, once per model or version of product, any publicly available technical design documentation and, under a reasonable, mutually-acceptable non-disclosure agreement, the service manual for such product, in order to assist in the evaluation of the compliance of such product with these Robustness Rules.

4.2 **Inspection and Report.** Upon a reasonable and good faith belief that a particular hardware model or software version of a Licensed Product designed or manufactured by Adopter does not comply with the Robustness Rules then in effect for such Licensed Product, and upon reasonable notice to Adopter via the Authority, the Association may request Adopter to submit promptly to an independent expert (acceptable to Adopter, which acceptance shall not be unreasonably withheld) for inspection such detailed information as Adopter deems necessary to understand such product's implementation of the Specification and Compliance Rules, such as would be sufficient to determine whether such product complies with these Robustness Rules. Adopter's participation in this inspection procedure is voluntary; no adverse inference may be drawn from Adopter's refusal of the Association's request or refusal to participate, in whole or in part, in such inspection. The conduct of such inspection and the contents of any report made by the independent expert shall be subject to the provisions of a nondisclosure agreement, mutually-agreeable to the Association, Adopter, and such expert, such agreement not to be unreasonably withheld, that also provide protections for Confidential Information and

Highly Confidential Information relating to SmartRight that are no less stringent than those provided for in this Agreement. Such examination and report shall be conducted at the sole expense of the Association. Nothing in this paragraph shall limit the role or testimony of such expert, if any, in a judicial proceeding under such protective orders as a court may impose. Adopter shall not be precluded or estopped from challenging the opinion of such expert in any forum; nor shall any party be entitled to argue that any greater weight or evidentiary presumption should be accorded to the expert report than to any other relevant evidence. This provision may not be invoked more than once per hardware model or software version, provided that such right of inspection shall include the right to re-inspect the implementation of such model or version if it has been revised in an effort to cure any alleged failure of compliance.

EXHIBIT C-1
ROBUSTNESS CHECKLIST

Notice: This Checklist is intended as an aid to the correct implementation of the Robustness Rules for hardware and software implementations of the SmartRight Specification in a Licensed Product. The Authority strongly recommends that you complete this Checklist for each hardware model or software version of a Licensed Product before releasing any product and at a sufficiently early date in design, as well as during production, to avoid product compliance redesign delays. This Checklist does not address all aspects of the Specification and completion of this checklist is not sufficient to establish Compliance. Failure to perform necessary tests and analysis could result in a failure to comply fully with the Specification, Compliance Rules or Robustness Rules in breach of Adopter Agreement and, as a consequence, in appropriate legal action.

Notwithstanding whether any particular design or production work is being outsourced or handled by contractors to the company, compliance with the above Rules remains the responsibility of this company.

DATE: _____
MANUFACTURER: _____
PRODUCT NAME: _____

HARDWARE MODEL OR SOFTWARE VERSION: _____
NAME OF TEST ENGINEER COMPLETING CHECKLIST:
TEST ENGINEER: _____
COMPANY
NAME: _____

COMPANY ADDRESS: _____
PHONE
NUMBER: _____

FAX NUMBER: _____

BER: _____

GENERAL IMPLEMENTATION QUESTIONS

1. Has the Licensed Product been designed and manufactured so there are no switches, buttons, jumpers, or software equivalents of the foregoing, or specific traces that can be cut, by which the content protection technologies, analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specification or Compliance Rules can be defeated or by which Protected Content can be exposed to unauthorized copying or use.?
2. Has the Licensed Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can intercept the flow of data or expose it to unauthorized copying?
3. Has the Licensed Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can turn off any analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specification or Compliance Rules?
4. Does the Licensed Product have service menus, service functions, or service utilities that can alter or expose the flow of data within the device?

If Yes, please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to expose or misdirect Decrypted SmartRight Content.

5. Does the Licensed Product have service menus, service functions, or service utilities that can turn off any analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specification or Compliance Rules?
If Yes, please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to defeat the

content protection features of SmartRight (including compliance with the Compliance Rules and the Specification).

6. Does the Licensed Product have any User Accessible Buses (as defined in Section 1.50 of the Robustness Rules)?

If so, is Protected Content carried on this bus?

If so, then: identify and describe the bus, and whether the Protected Content is compressed or uncompressed. If such Data is compressed, then explain in detail how and by what means the data is being protected as required by Section 2.2 of the Compliance Rules.

7. Explain in detail how the Licensed Product protects the confidentiality of all Keys.

8. Explain in detail how the Licensed Product protects the confidentiality of the confidential cryptographic algorithms used in SmartRight.

9. If the Licensed Product Protected Content from one part of the product to another, whether among software modules, integrated circuits or otherwise or a combination thereof, explain how the portions of the product that perform authentication and decryption and the MPEG (or similar) decoder have been designed, associated and integrated with each other so that Protected Content is secure from interception and copying as required in Section 3.1 of the Robustness Rules.

10. Are any SmartRight functions implemented in Hardware?

If Yes, complete hardware implementation questions.

11. Are any SmartRight functions implemented in Software?

If Yes, complete software implementation questions.

SOFTWARE IMPLEMENTATION QUESTIONS

12. In the Licensed Product, describe the method by which all Keys are stored in a protected manner.

13. Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices?

14. In the Licensed Product, describe the method used to obfuscate the confidential cryptographic algorithms and Keys used in SmartRight and implemented in software.

15. Describe the method in the Licensed Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules

or devices within a Licensed Product) are created and held in a protected manner.

16. Describe the method being used to prevent commonly available debugging or de-compiling tools (e.g., Softice) from being used to single-step, decompile, or examine the operation of the SmartRight functions implemented in software.

17. Describe the method by which the Licensed Product self-checks the integrity of component parts in such manner that modifications will cause failure of authorization or decryption as described in Section 3.2.2 of the Robustness Rules. Describe what happens when integrity is violated.

18. To assure that integrity self-checking is being performed, perform a test to assure that the executable will fail to work once a binary editor is used to modify a random byte of the executable image containing SmartRight functions, and describe the method and results of the test.

HARDWARE IMPLEMENTATION QUESTIONS

19. In the Licensed Product, describe the method by which all Keys are stored in a protected manner and how their confidentiality is maintained.

20. Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices?

21. In the Licensed Product, describe how the confidential cryptographic algorithms and Keys used in SmartRight have been implemented in silicon circuitry or firmware so that they cannot be read.

22. Describe the method in the Licensed Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Licensed Product) are created and held in a protected manner.

23. Describe the means used to prevent attempts to replace, remove, or alter hardware elements or modules used to implement SmartRight functions.

24. In the Licensed Product, does the removal or replacement of hardware elements or modules that would compromise the content protection features of SmartRight (including the Compliance Rules, the Specification, and the Robustness Rules) damage the Licensed Product so as to render the Licensed Product unable to receive, decrypt, or decode SmartRight Content?

Notice: This checklist does not supersede or supplant the SmartRight Specification, Compliance Rules, or Robustness Rules. The Company and its Test Engineer are advised that there are elements of the Specification and Compliance Rules that are

not reflected here but that must be complied with.

SIGNATURES:

Signature of Test Engineer with Personal Knowledge of Answers

Date

Printed Name of Test Engineer with Personal Knowledge of Answers